Universidad Nacional Mayor de San Marcos
Universidad del Perú. Decana de América

Dirección General de Estudios de Posgrado
Facultad de Ingeniería de Sistemas e Informática
Unidad de Posgrado

Gestión de riesgos de seguridad de la información para empresas del sector telecomunicaciones

TESIS

Para optar el Grado Académico de Magíster en Gobierno de Tecnologías de Información

AUTOR

Miguel Humberto HUAURA MERE

ASESOR

Dra. Nora Bertha LA SERNA PALOMINO

Lima, Perú

2019

Referencia bibliográfica

Huaura, M. (2019). *Gestión de riesgos de seguridad de la información para empresas del sector telecomunicaciones*. Tesis para optar grado de Magíster en Gobierno de Tecnologías de Información. Unidad de Posgrado, Facultad de Ingeniería de Sistemas e Informática, Universidad Nacional Mayor de San Marcos, Lima, Perú.

---

1. Código ORCID del Autor:
2. Código ORCID del Asesor: 0000-0002-4292-344X
3. Grupo de Investigación:
4. Institución que Financia la Investigación:
5. Ubicación Geográfica (Incluir Localidad y/o Coord. Geográficas): 150101
6. Año o rango de Años que abarco la investigación: 2014-2018
7. DNI: 42634060

Universidad Nacional Mayor de San Marcos
Universidad del Perú. Decana de América
Facultad de Ingeniería de Sistemas e Informática
Vicedecanato de Investigación y Posgrado
Unidad de Posgrado

SUSTENTACIÓN DE TESIS PARA OPTAR EL GRADO DE MAGÍSTER EN GOBIERNO DE TECNOLOGÍAS DE INFORMACIÓN

En la Ciudad Universitaria, a los quince (15) días del mes de julio del 2019, siendo las .19:22 horas, se reunieron en el Aula Magna de la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional Mayor de San Marcos, el Jurado de Tesis conformado por los siguientes docentes:

Mg. Zoraida Mamani Rodriguez (Presidente)
Mg. Javier Alfonso Seclén Arana (Miembro)
Mg. Julio César Rojas Medina (Miembro)
Dra. Nora Bertha La Serna Palomino (Asesora)

Se inició la Sustentación invitando al candidato a Magíster ***Miguel Humberto Huaura Mere,,*** *para que realizara la exposición oral y pública de la tesis para optar el Grado de Magíster en Gobierno de Tecnologías de Información, siendo la Tesis intitulada:*

"Gestión de Riesgos de Seguridad de la Información para Empresas del Sector Telecomunicaciones"

Concluida la exposición, los miembros del Jurado de Tesis procedieron a formular sus preguntas que fueron absueltas por el graduando; acto seguido se procedió a la evaluación correspondiente, habiendo obtenido la siguiente calificación:

.....17 MUY BUENO.....

Por tanto el Presidente del Jurado, de acuerdo al Reglamento General de Estudios de Posgrado, otorga al Bachiller ***Miguel Humberto Huaura Mere*** *el Grado de Magíster en Gobierno de Tecnologías de Información.*

Siendo las.20:12 hrs horas, el Presidente del Jurado de Tesis da por concluido el acto académico de Sustentación de Tesis.

Mg. Zoraida Mamani Rodriguez
(Presidente)

Mg. Javier Alfonso Seclén Arana
(Miembro)

Mg. Julio César Rojas Medina
(Miembro)

Dra. Nora Bertha La Serna Palomino
(Asesora)

DEDICATORIA:

En primer lugar doy gracias a Dios todopoderoso por guiarme y derramar sus bendiciones en todo momento y sobre todo por darme la energía para elaborar esta tesis.

A mis padres Miguel y Gladys por su apoyo constante y son ellos a quien les debo eternamente los logros obtenidos.

A mi hermano menor Robert por su apoyo permanente.

Para ellos es esta dedicatoria, a quienes les debo todo el apoyo recibido.

AGRADECIMIENTOS

Quiero expresar mi agradecimiento en primera instancia a Dios, porque si tú no intervienes, hoy no fuera posible este tan anhelado logro.

Un agradecimiento especial a la Universidad Nacional Mayor de San Marcos (UNMSM), a la Facultad de Postgrado de Ingeniería de Sistemas e Informática y docentes, por su dedicación en su trabajo y por la oportunidad de realizar esta tesis.

También, expresar mis agradecimientos al Dr. Carlos Pastor Carrasco y a la Dra. Nora La Serna Palomino, por estar siempre a disposición en brindarme su ayuda para llevar a cabo tan importante tema de investigación.

A mis padres Miguel Huaura y Gladys Mere, porque siempre estuvieron ahí en todo momento.

Gracias a mi hermano Robert, mis compañeros y amigos incondicionales.

Nuevamente gracias.

Índice General

Lista de Cuadros

Lista de Figuras

RESUMEN

La tesis titulada “Gestión de Riesgos de Seguridad de la Información para empresas del sector Telecomunicaciones” realizado en Lima Metropolitana entre los años 2014 y 2017, participaron las empresas del sector Telecomunicaciones, las variables de esta tesis son Gestión de Riesgos y Seguridad de la Información.

La presente tesis se justifica porque posee valor estratégico, de aplicación metodológica, relevancia social, financiera y legal, metodología de trabajo que genera aspectos positivos en el cumplimiento en diversos aspectos, tanto internos como externos.

Para realizar el análisis de los posibles riesgos de este sector, se ejecutó una encuesta de 10 preguntas validado por juicio de expertos. Una vez definida la metodología (soportado con estándares internacionales NTP ISO/IEC 31000 e ISO/IEC 27005) apoyado con herramientas informáticas como soporte a las actividades, para la eficiencia de este trabajo.

Finalmente, se enlistan las conclusiones y recomendaciones que permita demostrar la actitud de las empresas de la gestión deficiente e identificar de forma apropiada los riesgos asociados a la Seguridad de la Información y como ello termina afectando a los procesos y en los objetivos propuestos por la empresa.

Palabras Claves: Gestión de Riesgos, Seguridad de la Información, Norma Técnica Peruana, Empresas del sector Telecomunicaciones.

SUMMARY

The thesis entitled "Information Security Risk Management for companies in the Telecommunications sector" held in Lima Metropolitan between 2014 and 2017, participation of companies in the Telecommunications sector, the variables of this Thesis are Risk Management and Information Security.

This thesis is justified because it has strategic value, methodological application, social, financial and legal relevance, work that generates positive aspects in the fulfillment of various aspects, both internal and external.

To carry out the analysis of the possible risks in this sector, a survey of 10 questions was carried out, validated by expert judgment. Once the methodology has been defined (support supported for international standards NTP ISO / IEC 31000 and ISO / IEC 27005) supported by computer tools to support the activities, for the efficiency of this work.

Finally, list the conclusions and recommendations that allow you to demonstrate the attitude of companies of poor management and identify the form of the risks associated with information security and how it ends up affecting the processes and objectives proposed by the company.

Key Words: Risk Management, Information Security, Peruvian Technical Standard, Telecommunications sector Companies.

Capítulo 1 - INTRODUCCIÓN

1.1. Situación Problemática

Las empresas del sector Telecomunicaciones, enfrentan pérdidas económicas, por factores de índole interno o externo como es la pérdida de información, debido que los riesgos no se encuentran debidamente gestionados; estos riesgos pueden ser de origen conocido o desconocidos; la seguridad de la información en conjunto con la gestión de riesgos hacen que las empresas logren cumplir con sus objetivos.

En una publicación de ISACA Journal, el autor del artículo, Devassy (2016) hace mención "(…) En el pasado se han desencadenado diversas fugas de información que han terminado por paralizar a muchas organizaciones, que en muchos de los casos han generado daños irreparables. La incapacidad de poder de visualizar los efectos de la pérdida de información crítica puede dar lugar a importantes consecuencias (…)". (pág. 34)

En un artículo publicado por Wlosinski (2017 hace mención "Las causas principales de los incidentes de privacidad incluyen la subcontratación de datos, información privilegiada maliciosa, fallos del sistema, ataques cibernéticos y la falta de fragmentación o eliminación de datos de privacidad correctamente.". (pág. 36)

En un artículo publicado por Michael Werneburg (2017) hace mención: "Las vulnerabilidades de las aplicaciones tienen factores de riesgo cercanos y secundarios. Los factores de riesgo cercanos son evidentes: las infracciones de los datos afectan a las personas afectadas cuya información personal está comprometida. Pero el riesgo secundario radica en la exposición legal a la organización del cliente, es decir, el riesgo para la organización de servicios tecnológicos, cuyo producto permitió el incumplimiento, sería responsable. Las infracciones de datos con frecuencia dan lugar a acciones legales, es decir, acciones". (Werneburg, 2017, pág. 43)

Megias Terol, y otros, (2008) mencionan que "existen diversos desafíos o retos de carácter estructural a los que se enfrentan actualmente las organizaciones y que es importante conocer. Conocimiento es anticipación en este nuevo paradigma". (pág. 15).

En la publicación (PricewaterhouseCoopers, 2018) menciona, “Los delitos económicos y el fraude tienen mayor visibilidad en lo últimos años y no existe compañía invulnerable, independientemente de su tamaño. Según nuestro estudio (PricewaterhouseCoopers) el 55% de los encuestados peruanos manifiesta haber sido de este tipo de delitos en los últimos dos años, cifra que supera en 6 puntos porcentuales a la situación global”. (pág. 2)

Actualmente estas empresas se encuentran inspeccionadas por el Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL) “es un organismo público especializado, regulador y descentralizado adscrito a la Presidencia del Consejo de Ministros, que cuenta con autonomía técnica, administrativa, económica y financiera”. (Organismo Supervisor de Inversión Privada en Telecomunicaciones, 2018)

En la publicación de OCDE, 2018 hace referencia: “Del mismo modo, en el campo de las telecomunicaciones se introdujo un marco jurídico para realizar actividades en este sector. Este mercado se abrió y liberalizó. Todas las operaciones de este mercado se abrieron a la inversión nacional y extranjera. Se creó el Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL) para regular las tarifas y el comportamiento de las empresas privadas en este sector”. (pág. 38)

Adicional, las empresas (públicas o privadas) tienen por obligación cumplir la Ley de Protección de Datos Personales vigente desde el año 2011.

1.1.1. Diagrama de Ishikawa

Para poder tener mayor conocimiento y mejor entendimiento de los principales riesgos que afrontan las empresas de este sector de Telecomunicaciones se muestra el Diagrama de Ishikawa.

Véase el Anexos (9.1), página 109.

1.2. Formulación del Problema

1.2.1. Problema General

Luego de realizar un breve análisis de la situación problemática, se deriva la siguiente pregunta:

- ¿De qué manera la gestión de riesgos de seguridad de la información basada en la NTP ISO/IEC 31000 influye en el control de los riesgos en empresas del sector Telecomunicaciones?

1.2.2. Problemas específicos

Para tal efecto se determina los siguientes problemas específicos:

- ¿De qué manera la gestión de riesgos de seguridad de la información permite identificar los posibles riesgos de pérdida de información?
- ¿De qué manera la gestión de riesgos de seguridad de la información mejora la toma decisiones de la Alta Dirección?
- ¿De qué manera la gestión de riesgos de seguridad de la información permite generar rentabilidad a las empresas?

1.3. Justificación Teórica

El propósito de realizar una gestión de riesgo es, garantizar que los posibles riesgos de la seguridad de la información sean identificados, evaluados, tratados de manera oportuna.

Es necesario citar a Cano (2014), donde hace referencia sobre este tema: "Considerando los cambios en los modelos de negocio y los escenarios desafiantes planteados por los analistas, cumplir con el reto de anticiparse a los riesgos emergentes que afecten la confiabilidad de las operaciones y proteger el modelo de generación de valor de la empresa, se hace cada vez más desafiante y por lo tanto, motivador para mantenerse alerta y atento a los cambios que se plantean en la dinámica de las organizaciones". (pág. 1)

Las empresas manejan, procesan, almacenan y transfieren información valiosa de los clientes, patentes, personal, servicios, operaciones, otros.

La implementación o monitoreo de controles con respecto a los riesgos identificados, genera indicadores de gestión que son proporcionados a la Alta Dirección para seguimiento y posterior toma de decisiones para futuras inversiones.

Generar valor a la empresa a través del conocimiento de sus riesgos y evitar los incumplimientos o penalidades de los entes reguladores o parte legal.

Por ello la justificación de la tesis radica:

a) Porque el negocio se sustenta a partir de la información que maneja.
b) Porque no sólo la seguridad es un tema "tecnológico".
c) Porque la gestión de riesgos está presente en los procesos de las empresas.

1.4. Justificación Práctica

Con una correcta ejecución de gestión de riesgos de seguridad de la información se pretende identificar y controlar los riesgos de forma clara que permita a la Alta Dirección tomar adecuadas decisiones en función de su estrategia, con una base a una metodología de gestión de riesgos, con base en la NTP ISO/IEC 31000.

La tesis elaborada puede ser consultada por la Alta Dirección, Gerentes, Jefes, consultores y puede ser aplicada tanto a procesos, activos de información, de manera general aborda a toda la empresa desde la parte estratégica hasta la parte operativa.

Adicional, la Gestión de Riesgos de Seguridad de la Información, está investigación es orientada al sector Telecomunicaciones, es necesario precisar que puede ser implementada por cualquier tipo de empresa independiente a su rubro o giro de negocio, tomando en consideración ciertos requisitos para su cumplimiento y eficiencia.

En la publicación de PricewaterhouseCoopers, (2018) hace referencia: "Todos hemos oído hablar de la importancia de la seguridad informática y como esta asume un rol principal cada que se discuten innovaciones tecnológicas o aspectos de la era digital". (pág. 6).

Adicional, es preciso hacer énfasis a lo comentado por PricewaterhouseCoopers, (2018) es necesario incluir los temas relacionados con ciberseguridad.

Es por ello, el investigador busca enfocarse en las problemáticas que afrontan las empresas del sector del Telecomunicaciones y brindar un aporte que genere líneas de acción que permita prevenir y/o corregir estas problemáticas y brindar recomendaciones rápidas y eficientes para mitigar el impacto a los riesgos o las posibles consecuencias, como por ejemplo el incumplimiento de las leyes y regulaciones vigentes.

1.4.1. Objetivos de la Investigación

1.4.2. Objetivo General

Determinar que la gestión de riesgos de seguridad de la información basada en la NTP ISO/IEC 31000 influye en el control de los riesgos en empresas del sector Telecomunicaciones.

1.4.3. Objetivos Específicos

1. Identificar los posibles riesgos de pérdida de información a través de una gestión de riesgos de seguridad de la información.
2. Obtener como mejora la toma de decisiones de la Alta Dirección a través de una gestión de riesgos de seguridad de la información.
3. Generar rentabilidad de las empresas a través de una gestión de riesgos de seguridad de la información.

1.5. Hipótesis

1.5.1. Hipótesis general

- Una gestión de riesgos de seguridad de la información basada en la NTP ISO/IEC 31000 en las empresas del sector Telecomunicaciones influye en el control de los riesgos de seguridad de la información.

1.5.2. Hipótesis específicas

- Realizando una gestión de riesgos de seguridad de la información identifica los posibles riesgos de pérdida de información.
- Realizando una gestión de riesgos de seguridad de la información mejora la toma de decisiones de la Alta Dirección.
- Realizando una gestión de riesgos de seguridad de la información genera rentabilidad en las empresas.

1.6. Matriz de Consistencia

La construcción de una Matriz de Consistencia, permite el análisis e interpretación de la tesis, en el cual muestra en conjunto: el problema, objetivos, hipótesis, variables y otros.

Véase Anexos 9.2, página 110.

Capítulo 2 - MARCO TEÓRICO

El siguiente punto trata, con mayor detalle el tema de investigación, donde se citará los aportes de diversos autores, permitirá al lector y otros investigadores una idea fundamentada sobre el tema abordado, indicados a continuación:

- Antecedentes de la Investigación
- Bases teóricas
- Marcos conceptuales

2.1. Antecedentes de la Investigación

En cuanto a los antecedentes de la investigación, se presenta varios estudios, detallados a continuación:

2.1.1. Tesis "Impacto del riesgo en el gobierno de tecnologías de información y comunicación en la gestión empresarial industrial del siglo XXI"

En la tesis de Pastor (2010), en su trabajo de investigación toma como objetivo: "Identificar en qué medida la implementación de un sistema de gestión del riesgo dentro del gobierno de TIC en la gestión de los procesos contribuirá en la creación de ventajas competitivas en la gestión de los procesos de las organizaciones industriales del sector metal mecánico". (pág. 31)

Pastor (2010), menciona que:

En el trabajo de investigación hace énfasis a la falta de un Gobierno de Tecnologías de Información, el permita un alineamiento e integración entre el Gobierno y el negocio. Además, hay que mencionar dentro de los problemas expuestos, la ausencia de una visión técnica – tecnológica originando como consecuencia el incremento de gastos de TIC's.

Se debe agregar que, otro de los problemas es la ausencia de gerencia en TIC y otro problema no menos importante que afecta a las Gerencias Generales es la falta de incorporación de las TIC en la estrategia de negocio y solo se mide el riesgo de modo parcial.

Es necesario mencionar que el instrumento de recolección de datos fue: cuestionario.

Pastor (2010), indica como conclusión:

(…) “La aportación de las TI a la generación de valor, en su sentido más amplio, se convierte actualmente en uno de los temas que generan mayor interés dentro de la investigación en gestión empresarial”. (pág. 192)

Acorde con, la investigación de Pastor (2010), es pertinente mencionar que efectivamente los problemas y las conclusiones derivadas tienen relación con la presente tesis, definitavamente en las empresas del sector Telecomunicaciones muchas veces carecen de una adopción de gestión de riesgos que incorporen a las TIC como parte de su estrategia técnica- tecnologica y táctica, de la misma manera ocurre al involucramiento de la gestión de riesgos enfocado a la seguridad de la información, para la protección de los activos de la empresa.

Dicho brevemente, de existir una visión de gerencia de TIC, es probable que se obtenga una gestión orientada al Gobierno de TI y el negocio.

2.1.2. Tesis “Caracterización y análisis de riesgos de la gestión tecnológica de la Universidad del Valle”

En la tesis Zambrano & Caro (2013)**,** toma como objetivo “Realizar la caracterización de la situación Actual de la gestión tecnológica de la Universidad del Valle.”. (pág. 17)

Zambrano & Caro (2013) detallan como problema en el cual identifica como problema: “(…) la necesidad de realizar una caracterización de los diferentes actores y de la situación actual de la plataforma tecnológica de la Universidad del Valle, que nos conduzca a elaborar un modelo de gestión tecnológica que permita mejorar la gestión de las tecnologías en la Universidad.” (Zámbrano Castillo & Caro Perea, 2013, págs. 15-16)

Como mencionan los autores, el factor tecnológico es cada vez más importante como soporte a los procesos, también es importante señalar que este factor es cada vez más es considerada como parte de la estrategia de las empresas, con la diferencia que esta investigación es orientada al sector educativo.

Zambrano & Caro (2013)**,** toma como parte de sus conclusiones, la gestión en temas tecnológicos debería estar integrada con la plana estratégica, en donde coincide con Pastor (2010) en este punto, además los autores consideran importante la inclusión del recurso humano, auditorías entre otros aspectos.

2.1.3. Tesis “Marco para el Gobierno de la Seguridad de la Información en servicios Cloud Computing”

En la tesis de Martínez (2014), toma como objetivo “Definir un proceso que sistematice el gobierno de la seguridad de los servicios Cloud Computing”. (pág. 52)

Martínez (2014), toma parte de los problemas de su investigación hace referencia “Los dispositivos móviles, tales como los teléfonos inteligentes smartphones, tabletas u ordenadores portátiles, están incrementando muy rápidamente su rendimiento, alcanzando en muchos casos una capacidad comparable a la de un ordenador tradicional, lo que les facilita alcanzar grandes tasas de penetración a un ritmo vertiginoso”. (pág. 227)

Indiscutiblemte, Martínez (2014), aborda un problema que representa en algunas empresas factores de riesgos (posible fuga o pérdida de información) el uso de teléfonos inteligentes, mientras para otras una oportunidad de mejora. Para efectos de la presente tesis es un tema sensible, por diversos motivos, comenzaré dando un ejemplo, en las empresas del sector Telecomunicaciones al manejar información sensible de los usuarios, al suceder el robo o sustracción de un dispositivo móvil (de uso personal o asignado por la empresa),es probable que la información contenida sea accedida por personas no autorizadas y puedan usar dicha información para fines lucarativos (venta al mercado informal o a la competencia).

Martínez (2014) hace referencia al instrumento de recolección de datos el uso de entrevistas y cuestionarios con el personal involucrado. (Rebollo Martínez, 2014, pág. 205)

Martínez (2014) hace mención como parte de las conclusiones: “Todas estas tareas están estructuradas a lo largo del ciclo de vida de los servicios Cloud Computing que ha sido identificado, e incorporan los aspectos de seguridad más destacados existentes en los estándares y mejores prácticas disponibles en la actualidad.” (pág. 290)

Sin embargo, con la evolución y los constantes cambios ya existe mayor información e investigaciones sobre este tema, no es parte de esta tesis profundizar sobre “cloud computing”, pero si es necesario precisar que las empresas de este rubro deberían considerar en su mapa de riesgos, este tipo

de tecnología actualmente es tomado por las empresas debido a las ventajas que representa.

2.1.4. Tesis "Factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001".

En la tesis de Seclen (2016), toma como objetivo: "El objetivo de esta investigación es analizar las principales limitaciones y problemas que vienen enfrentando las entidades del sector público en la implementación del SGSI, (…)" (pág. 6)

Seclen (2016), hace referencia como problema "¿Cuáles son los factores que afectan la implementación del Sistema de Gestión de Seguridad de la Información en las Entidades Públicas Peruanas?" (pág. 3)

Seclen (2016), toma como instrumentos de recolección de datos "En este capítulo se presenta el diseño de la estrategia de la tesis cualitativa, la cual está basada en la recolección de datos a través de herramientas tales como entrevistas y observaciones realizadas con el apoyo de propio investigador como instrumento principal". (pág. 79)

Seclen (2016), hace mención como conclusión: "Actualmente, las entidades -tanto públicas como privadas- vienen enfrentando desafíos, en este ámbito, los cuales se han tornado más sofisticados y pueden llegar a ser potencialmente devastadores. Por ello, esta política estratégica debe incluir un acompañamiento en la gestión y la definición de sus procesos en cada una de las organizaciones involucradas". (pág. 172)

Dicho lo anterior, considero que en actualidad se tiene mayor inclusión la seguridad de la información en el interior de las empresas (en esta investigación para sector público), pero resulta insuficiente debido a la ausencia de profesionales especializados o con el suficiente conocimiento en el tema, por ejemplo un Jefe u Oficial de Seguridad de la Seguridad, el autor Seclen lo toma en consideración (aspecto importante). Además, en la presente tesis se hace mención de la inclusión de esta figura de gestión.

Además, es importante mencionar la necesidad de del cumplimiento de Política, como eje para alcanzar los objetivos estratégicos.

2.1.5. Tesis “Elaboración de una guía de gestión de riesgos basados en la norma NTC-ISO 31000 para el proceso de gestión de incidentes y peticiones de servicio del área de mesa de ayuda de empresas de servicios de soporte de tecnología en Colombia”

En la investigación de Arias, Díaz & Vargas, (2014) coinciden como objetivo, “Elaborar una guía de gestión de riesgos basados en la norma NTC-ISO 31000, para el proceso de gestión de incidentes y peticiones de servicio del área de mesa de ayuda, de empresas de servicios de soporte de tecnología en Colombia”. (pág. 20)

Arias, Díaz & Vargas, (2014) consideran como parte de los problemas identificados: “Las tecnologías se han convertido en una herramienta para la mayoría de las actividades que realiza un ser humano, como tomar una foto hasta comunicaciones de larga distancia que en otras circunstancias habrían demandado bastante tiempo. La tendencia actual es el uso de la misma en las organizaciones como apoyo a la disponibilidad y gestión de información, permitiendo programar gastos, compras o la toma de decisiones importantes que definen el rumbo de la compañía.” (pág. 17)

La gestión de incidentes es un proceso que permite identificar posibles errores, inconsistencias, desviaciones o posibles eventos que puedan causar algún impacto. Es por ello, la implementación de métricas e indicadores permiten evidenciar algún tipo de anomalía que podría originar algún tipo de riesgo en las empresas.

Arias, Díaz & Vargas, (2014) toman diversas fuentes de información que son: entrevistas, estadísticas, documentación obtenida de los procesos y subprocesos.

Arias, Díaz & Vargas, (2014) coinciden como parte de sus conclusiones: “En todo proceso, área u organización siempre existirán riesgos, independientemente si estos son detectados o no, y es por este motivo que se debe implementar una gestión de riesgos eficiente para mitigarlos pues eliminarlos no es posible pero si ejercer un control adecuado sobre estos.”. (pág. 64)

De acuerdo, con los autores coincido en su afirmación sobre la existencia de riesgos, razón por la cual las empresas deben estar en permanente estado de

"alerta", a fin de evitar efectos adversos en sus procesos y contar con personal capacitado.

2.1.6. Tesis "Estudio para el desarrollo de un modelo de Gestión de Riesgos y Seguridad de la Información para instituciones militares".

Estévez (2014) plantea como objetivo "(…) proponer un Modelo de Gestión de Riesgos y Seguridad Informática, para la detección y mejoramiento administrativa de la seguridad en general de las instituciones militares, que analizados para un mejor análisis y gestión servirán para aplicarlas y tener un mejor respaldo que poseen las misma". (págs. 14-15)

Estévez (2014) menciona como parte de los problema, "Estos sistemas de información son vulnerables a una diversidad de amenazas y atentados por parte de personas que pueden o no pertenecer a la institución, ya sea por: desastres naturales, a causa de intromisiones, o por errores humanos (de utilización y negligencia personal), o amenazas provocadas (robo, fraude, sabotaje o interrupción de actividades de cómputos) (…)". (pág. 11)

Estévez (2014) menciona como parte de sus conclusiones:

"Considerando las dos metodologías de gestión de riesgos, Magerit y Octave, se ha demostrado que se puede obtener una fusión de ellas, en lo que sirve de base para el desarrollo de un nuevo modelo de gestión de riesgos y seguridad de la información, donde se logró la inclusión de los elementos importantes de cada una y se aproximó al problema de analizar los riesgos (…).". (pág. 166)

Como, menciona Estévez (2014), considero importante resaltar que parte de los problemas que afrontan las empresas del sector de Telecomunicaciones es la poca capacitación del factor humano, en temas relacionados a la seguridad de la información, desde el momento de la contración y durante el empleo, una buena practica es impartir capacitaciones y entrenamiento en este tema, por lo menos una o dos veces al año, este aspecto es esencial para que el usuario tome razón de la importancia de sus funciones y su contribución a evitar posibles riesgos que podrían repecutir en la confidencialidad e integridad de la información.

2.2. Bases Teóricas

El presente trabajo de investigación tiene como objetivo determinar que la gestión de riesgos de seguridad de la información basada en la NTP ISO/IEC 31000 influye en el control de los riesgos en empresas del sector Telecomunicaciones, por tanto en el presente acápite se detalla los diversas marcos de referencia que permiten garantizar una correcta y eficiente gestión de riesgos.

En el Figura 1 se muestra "Relaciones entre los componentes del marco de trabajo de la gestión del riesgo" (Norma Técnica Peruana NTP-ISO/IEC 31000:2011, 2011 Revisada 2016, pág. 12), que comprende las actividades e interacciones para aplicar de manera correcta el proceso de gestión de riesgos.

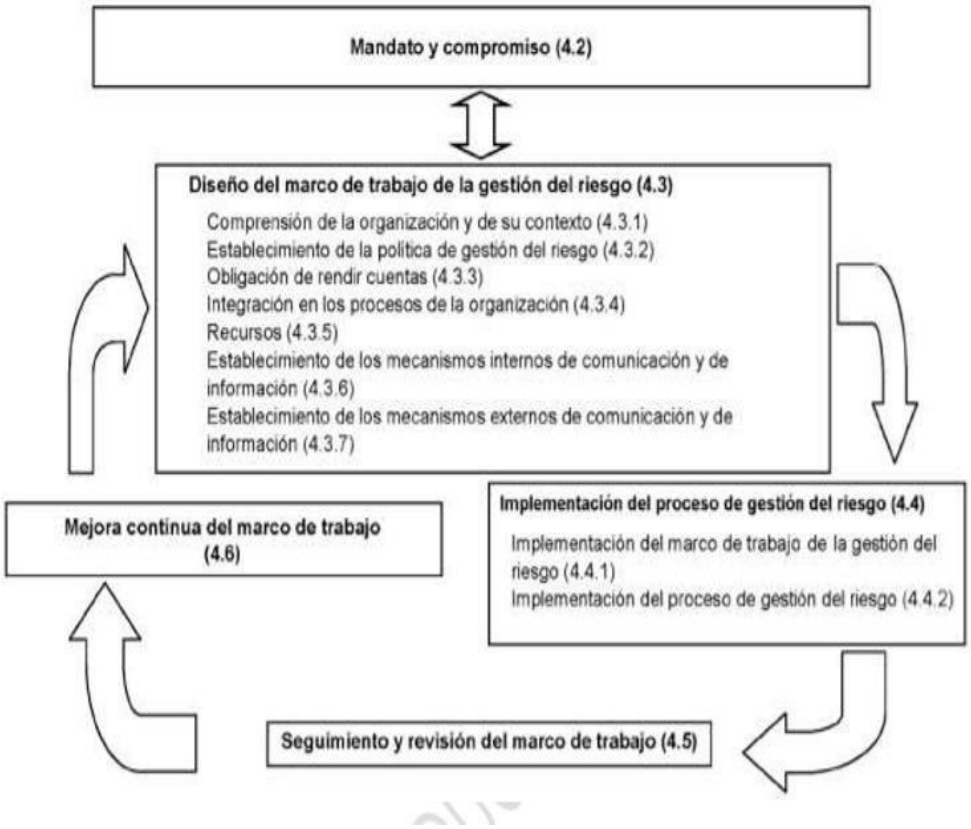


Figura 1: Relaciones entre los componentes del marco de trabajo de la gestión del riesgo

Fuente: (Norma Técnica Peruana NTP-ISO/IEC 31000:2011, 2011 Revisada 2016)

2.2.1. NTP ISO/IEC 31000

La NTP-ISO/IEC 31000:2011, es un estandar internacional que se orienta a la administración de riesgos, en el Perú es adoptada como Norma Técnica Peruana, con su última actualización en el año 2016; se enfoca a organizaciones de todos los tipos y tamaños a fin de protegerse y conseguir el cumplimiento de sus objetivos.

La NTP-ISO/IEC 31000:2011, hace mención:

"Todas las actividades de una organización implican riesgos. Las organizaciones gestionan el riesgo identificándolo, analizándolo y evaluando después si el riesgo se debería modificar mediante un tratamiento que satisfaga sus criterios de riesgo." (Norma Técnica Peruana NTP-ISO/IEC 31000:2011, 2011 Revisada 2016, pág. s.n)

La NTP-ISO/IEC 31000:2011, al ser adoptada por las empresas, conlleva a una serie de mejoras, es necesario mencionar para que estas mejoras se materialicen es necesaria la participación activa de la Alta Dirección, entre sus principales aportes, para efectos de la presente tesis son:

- Cumplimiento de los requisitos legales y reglamentarios aplicables para las empresas de Telecomunicaciones.
- Aumentar la probabilidad de cumplimiento de objetivos.
- Permitir la identificación de oportunidades y amenazas.

Según la NTP-ISO/IEC 31000:2011 hace referencia: "Esta Norma Técnica Peruana puede utilizarse por cualquier empresa pública, privada o social, asociación, grupo o individuo. Por tanto, esta Norma Técnica Peruana no es específica de una industria o sector concreto". (Norma Técnica Peruana NTP-ISO/IEC 31000:2011, 2011 Revisada 2016)

En la publicación de Casares, (2014), el autor hace mención:

> La gestión eficaz de los riesgos que amenazan a la empresa, mediante el uso de mapas de riesgo que la misma debería implementar, a medio plazo, para garantizar en el futuro, de este modo, sus objetivos estratégicos. (Casares San José - Martí, 2014, pág. 31)

2.2.2. Proceso de gestión de riesgos

Según, Casares & Lizarzaburu (2016) consideran:

> "El proceso de gestión de riesgo debería ser una parte integral de la gestión y estar adaptado al proceso de negocio de la organización, recogiendo la

cultura y prácticas. Esto incluye los 5 componentes de establecimiento del contexto: evaluación de riesgo con la identificación, análisis y evaluación cualitativa y cuantitativa de los riesgos; el tratamiento del riesgo para la toma de decisiones; la comunicación y consulta; el monitoreo y revisión". (Casares San José Martí & Lizarzaburu, 2016, pág. 51)

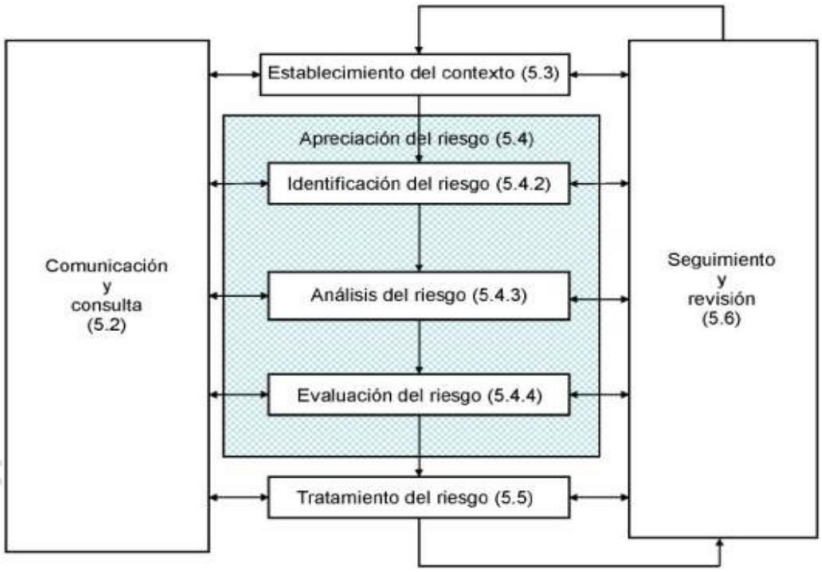


Figura 2: Proceso de gestión del riesgo

Fuente: (Norma Técnica Peruana NTP-ISO/IEC 31000:2011, 2011 Revisada 2016)

Casares & Lizarzaburu (2016) coincide en su publicación los aportes de la ISO/IEC 31000, como lo muestra la Figura 2, toma en consideración los siguientes puntos :

- **Establecimiento del contexto**

  En esencia, el punto principal de este punto, es identificar los criterios de decisión, ponderar los criterios de evaluación de riesgos y fundamentalmente el establecimiento de las responsabilidades, objetivos y metas; y la visión que tiene la empresa respecto al alcance de la gestión de riesgos de seguridad de la información. (Casares San José Martí & Lizarzaburu, 2016, pág. 51)

Casares & Lizarzaburu (2016) consideran:

- **Contexto externo**

> Los autores mencionan, los aspectos relevantes en el contexto externo, es decir la identificación de los temas legales y regulatorios que están sujetas las empresas, en lo que respecta para tesis mencionaremos dos puntos que son afectados directamente: Ley del Secreto de las Telecomunicaciones y la Ley de Protección de Datos Personales.
>
> Entre otros aspectos a consideran son: Ambiente social y cultural, ambientes políticos, tecnológicos, entre otros. (Casares San José Martí & Lizarzaburu, 2016, pág. 52)

Casares & Lizarzaburu (2016) coinciden:

- **Contexto interno**

  Se toma en cuenta las Políticas y Procedimientos corporativos existentes, las personas, áreas o involucrados en la gestión de riesgos, se toma en cuenta la capacidad del factor humano, así como la definición de los roles y responsabilidades que se tendrá que asumir. (Casares San José Martí & Lizarzaburu, 2016, pág. 52)

Casares & Lizarzaburu (2016) consideran:

> Hay que destacar, en este punto corresponde a la etapa de identificación de los riesgos y sus impactos, así como también conlleva a evaluar las posibles causas y efectos de los posibles impactos de los riesgos. (Casares San José Martí & Lizarzaburu, 2016, pág. 52)

Casares & Lizarzaburu (2016) coinciden:

- **Análisis de Riesgos**

  Recopilando lo más importante en el análisis de riesgos, "(…) su realización se puede dar con diversos grados de detalle dependiendo de varios factores como el riesgo, propósito del análisis e información, datos y recursos disponibles". (pág. 52)

  Por otra parte, considero adicionar otro concepto sobre la el análisis de riesgo, realizar un inventario de activos, para determinar la probabilidad de exposición frente a las amenazas y sus posibles impactos. (INCIBE - Instituto Nacioanl de Ciberseguridad, 2015)

Casares & Lizarzaburu (2016) coinciden en la evaluación de reisgos:

En el caso de, evaluación de riesgos es un punto crítico debido, donde la Alta Dirección tiene la responsabilidad de determinar qué riesgos necesitan tratamiento y prioridad o sencillamente salir del proceso, es decir no tratar el riesgo, esta decisión es previamente analizado de acuerdo a los impactos legales y otros que podrían afectar negativamente a las empresas. (Casares San José Martí & Lizarzaburu, 2016, pág. 52)

Casares & Lizarzaburu (2016) coinciden en el tratamiento de riesgos:

> En resumen, es la ejecución de unos criterios para el tratamiento de riesgos, que son:
>
> - Evitar el riesgo: Salir del proceso o actividad.
> - Compartir el riesgo: Transferir el tratamiento del riesgo a un tercero o proveedor.
> - Retener o mitigar el riesgo: Implementar controles para controlar o minimizar el riesgo.
> - Aceptar el riesgo: Esta decisión se basa si el riesgo no origina pérdidas sustanciales o el costo de la implementación del control resulta elevado. (Casares San José Martí & Lizarzaburu, 2016, pág. 53)

Casares & Lizarzaburu (2016) coinciden en la comunicación y consulta "(…) consulta con las partes involucradas en todas las etapas del proceso (…)". (pág. 53)

Casares & Lizarzaburu (2016) coinciden con respecto al monitoreo, asimismo sobre la revisión:

Está orientada en revisar si existen cambios sustanciales en la administración de riesgos, nuevas amenazas, cambios en el contexto interno y externo, cambios legales o identificación de nuevos riesgos. (Casares San José Martí & Lizarzaburu, 2016, pág. 53)

Todas las actividades referidas, deben ser revisadas a fin de evitar cambios inesperados en el proceso de gestión.

2.2.3. ISO/IEC 27005

Mientras la ISO/IEC 31000 es un marco internacional genérico para la gestión de riesgos, la ISO/IEC 27005 también, es un marco internacional con

la diferencia, que está orientado a la gestión de riesgos de seguridad de la información.

> Es importante mencionar que existen una serie de metodologías para realizar una gestión de riesgos, por tanto queda a criterio de la empresa o consultar la metodología que crea adecuada. La (ISO/IEC 27005:2011) considera: "(…) Una serie de metodologías existentes se puede utilizar en el marco descrito en esta norma internacional para implementar los requisitos de un SGSI. (ISO/IEC 27005:2011, 2011, pág. s.n)

La (ISO/IEC 27005:2011) considera:

> "La gestión del riesgo de seguridad de la información debe ser un proceso continuo. El proceso debe establecer el contexto externo e interno, evaluar los riesgos y tratar los riesgos utilizando un plan de tratamiento de riesgos para aplicar las recomendaciones y decisiones (…)". (ISO/IEC 27005:2011, 2011, pág. 6)

2.2.4. CSX Cybersecurity

En el libro Cybersecurity Fundamentals Study Guide, 2nd Edition, hace mención:

> Los términos "ciberseguridad" y "seguridad de la información" a menudo se usan indistintamente, pero en realidad, la ciberseguridad es una parte de la seguridad de la información. Más específicamente, la ciberseguridad se puede definir como la protección de los activos de información abordando las amenazas a la información procesada, almacenada y transportada por sistemas de información interconectados. (ISACA, 2017, pág. 11)

En el libro Cybersecurity Fundamentals Study Guide, 2nd Edition, hace mención sobre el riesgo:

> El deber central de la ciberseguridad es identificar, mitigar y gestionar los riesgos cibernéticos de los activos digitales de una organización. Ciberriesgo es la parte de la gestión de riesgos general que se centra únicamente en el riesgo que se manifiesta en el ciber (Entornos de información interconectados) del dominio. Mientras que la mayoría de las personas tienen una comprensión inherente del riesgo en sus vidas cotidianas, es importante comprender el riesgo en el contexto de la

> ciberseguridad, lo que significa saber cómo determinar, medir y reducir el riesgo de forma efectiva. (ISACA, 2017, pág. 25)

Efectivamente, si bien es cierto que ambos términos se relacionan, conviene resaltar que Seguridad de Información es un tema que tiene una mayor complejidad que no solo incluye activos digitales, sino también activos físicos e intangibles. Por otra parte, en el Perú aún existe una confusión entre ambos términos.

También, hace mención:

> Con demasiada frecuencia, los controles de Ciberseguridad se implementan con poca o ninguna evaluación del riesgo. Encuesta mundial de ISACA, la gerencia de TI, los auditores y los gerentes de seguridad demostraron que más del 80 por ciento de las compañías creen que los riesgos de seguridad son desconocidos o solo se evalúan parcialmente "y que" el analfabetismo de riesgo de TI y la falta de conciencia" son los principales desafíos en la gestión del riesgo. Por lo tanto, comprender los riesgos y las evaluaciones de riesgos son requisitos críticos para cualquier profesional de la seguridad. (ISACA, 2017, pág. 25)

Adicional, hace mención, “Un escenario de riesgo es una descripción de un posible evento cuya ocurrencia tendrá un impacto incierto en el logro de los objetivos de la empresa, que pueden ser positivos o negativos”. (ISACA, 2017, pág. 28)

2.2.5. COBIT 5

ISACA (2012), considera:

En su publicación analiza sobre la importancia de la información, su ciclo de vida (desde su creación hasta su destrucción) siendo un activo clave y vital para el negocio y como esta información se apoya en la tecnología para mantener su integridad y protección en el tiempo. (ISACA, 2012, pág. 13)

Además señala, “COBIT 5 provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas. Dicho de una manera sencilla, ayuda a las empresas a crear el valor (…)”. (ISACA, 2012, pág. 13)

Figura 3: Principios de COBIT 5

Fuente. (ISACA, 2012, pág. 13)

En el Anexo 9.3 (página 111), se detalla la Guía profesional general de los riesgos de TI, tomada de Cobit 5 para abordar los riesgos.

2.2.6. COSO - Committee of Sponsoring Organizations of the Treadway Commission

COSO (2017), establece entre sus beneficios, identificar y gestionar el riesgo en toda la entidad, para efectos de la presente tesis, es preciso mencionar que COSO hace un análisis integral a toda entidad u organización, porque "A veces el riesgo puede originarse en un parte de la entidad, pero puede afectar a otra parte diferente". (COSO - Committee of Sponsoring Organizations of the Treadway Commission, 2017, pág. 7)

Se debe agregar que, COSO (2017), considera como factor clave en la gestión del riesgo "la estrategia", asociado a la misión y visión. Además, se integra con otros aspectos de la empresa, así por ejemplo el gobierno corporativo, la gestión del desempeño y las prácticas de control interno. (COSO - Committee of Sponsoring Organizations of the Treadway Commission, 2017, págs. 4-5)

Por otro lado, es importante mencionar que COSO (2017) a comparación de la ISO/IEC 31000 toma un componente esencial de gestión, el gobierno y cultura, debido que el gobierno enfatiza la gestión del riesgo, mientras la cultura se refleja en la toma de decisiones. (COSO - Committee of Sponsoring Organizations of the Treadway Commission, 2017, pág. 21)

2.2.7. Otros aportes de autores

En las conclusiones de la investigación de Estévez (2014), indica "Se seleccionó Magerit, ya que sigue la terminología de la ISO 31000; donde centra un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de información". (pág. 166)

Dicho de otra manera, el autor considera que independientemente a la metodología seleccionada, en esencia se basa en el estándar internacional ISO/IEC 31000, por ser una metodología aplicable en diferentes o rubros de empresas.

En la tesis de Freire Zapata (2014) señala en su investigación sobre el beneficio y el aporte de un Modelo de Gestión de Seguridad de la Información en la empresa en la cual el autor realizó su investigación, como resultado señala con relación a los empleados, "(…) pueden acceder a la información de la empresa con la respectiva autorización, con esto la empresa considera a la información como un activo más, y minimiza el riesgo de fuga y/o pérdida de información". (Freire Zapata, 2014, pág. 110)

E&Y (2018), menciona:

> La cultura de riesgos en una organización se traduce en las acciones que realizan las personas que la integran para gestionar sus riesgos de negocio. Esta conecta la cultura más general de una organización con sus actividades de riesgo o de control de riesgos. Los reguladores a nivel mundial han enfatizado que la cultura se ha vuelto el aspecto más importante para abordar lo que ellos consideran como grandes fallas de conducta y de control que pueden tener un impacto sistemático si no se les aborda adecuadamente. Esto crea desafíos prácticos en su implementación y puede ser que los cronogramas designados necesiten soluciones tácticas a corto plazo. (Ernst & Young, 2018, pág. 93)

2.2.8. Seguridad de la Información

Actualmente uno de los factores más importantes que se debe tener en cuenta en todo tipo de organizaciones es la seguridad de la información, ya que los incidentes comprometen los activos de las empresas y las ponen en riesgo, lo anterior genera la necesidad de implementar sistemas o controles de seguridad a partir de un análisis de riesgos y minimizar así consecuencias no deseadas.

Es necesario precisar, la seguridad de la información como concepto básico, tiene como eje principal salvaguardar, proteger y maximizar el valor de los activos tangibles e intangibles de la empresa, se fundamenta en tres factores principales primordiales, como la confidencialidad, integridad y disponibilidad, estos conceptos se encuentran detallados en el punto 2.3 (Marcos Conceptuales).

La ISO/IEC 27002:2013, (2013), menciona "En un mundo interconectado, la información y los procesos relacionados, los sistemas, las redes y el personal involucrado en la operación, manejo y protección son activos que, como otros activos importantes del negocio, son valiosos para la empresa y, por consiguiente, merecen o necesitan protección contra diversos riesgos". (pág. 6)

Pallas (2009), el autor considera "La Seguridad es un proceso continuo, y como tal, se requiere de un sistema que lo soporte, que requiere además de su definición e implementación, ser mantenido y mejorado acorde a la evolución de las necesidades". (pág. 21)

La ISO/IEC 27002:2013, (2013), establece:

> Esta Norma Internacional proporciona directrices para los estándares de seguridad de la información de la organización y prácticas de gestión de la seguridad de la información, incluyendo la selección, aplicación y gestión de los controles teniendo en cuenta los riesgos para la seguridad de la información de la organización ambiente(s).
>
> Esta Norma Internacional está diseñado para ser utilizado por organizaciones que pretenden: Implementar un SGSI, otra razón salvaguardar o implementar controles a sus activos o procesos tomando como referente la Norma o simplemente por brindar un valor adicional

(ventaja competitiva) a sus clientes o proveedores. (ISO/IEC 27002:2013, 2013, pág. 8)

También, es necesario tomar en consideración la seguridad informática, que se orienta a la protección de activos tecnológicos y a su vez es importante dedicar algunas líneas a unas de las ramas de las tecnologías de información (hacking ético o ethical hacking), se considera como una actividad previa autorización del dueño del activo, especialistas de esta rama ejecuten diversas técnicas de ataque, con la finalidad de vulnerar la seguridad tecnológica, brindar informes de las brechas identificadas y brindar posibles soluciones, tanto a los desarrolladores, analistas y en general a las personas con poder de decisión. Añadir, la distinción lingüística en el término hacker, puesto que suele dársele una connotación negativa al relacionarlo como un tipo cibercriminal. (Di Lorio, y otros, 2017, págs. 116-117)

2.2.9. ISO/IEC 27001

Martínez (2014), el autor toma en consideración con respecto a la Seguridad de la Información, para su correcta implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) es validar la ejecución y/o cumplimiento del Ciclo de Deming (Plan-Check-Do-Act). (Rebollo Martínez, 2014, pág. 64)

Pallas (2009), el autor aborda el tema de la seguridad de la información como un factor estrategico y primordial en toda entidad. Dicho lo anterior, el autor señala "(…) Por lo tanto, debe primar un criterio de optimización de la relación Costo/ Beneficio: minimizar los riesgos, maximizando el logro de los objetivos sin salirse de los parámetros de niveles de inversión (presupuesto) de acuerdo a las prioridades establecidas por la Organización/ Empresa". (pág. 22)

Freire (2014), el autor considera para garantizar el salvaguarda de los activos de información en una empresa o entidad, es vital el ejercicio de estos pilares de la seguridad, los cuales son la confidencialidad, integridad y disponibilidad de la información. (Freire Zapata, 2014, pág. 18)

Es preciso destacar, en los diversos autores Martínez, Pallas y Freire coinciden parcialmente que la seguridad de la información como un proceso

interactivo, que se basan en tres pilares esenciales que definen a la seguridad de la información en: Confidencialidad, integridad y disponibilidad y el autor de la presente tesis en conformidad de los antecesores, también considera la importancia de la inclusión de la trazabilidad o auditabilidad, desde el punto de vista, de la necesidad de tener identificado todas las actividades que se realizan a nivel de usuarios o aplicaciones, ya sea por medios manuales o automatizados.

Por otro lado, sería bueno abordar un tema que no es parte del alcance de esta tesis, es la función de la auditoría dentro de las empresas de este sector, en el cual su contribución genera un apoyo transversal a las empresas, dando por ejemplo al soporte al buen gobierno, la gestión de riesgos. Habría que decir también, el auditor interno tiene la posición de evaluar el enfoque de privacidad e identificar riesgos significativos, que algunos casos podría estar orientado a la seguridad de la información, brindando un apoyo a los profesionales que tiene la responsabilidad de velar por los activos de información de las empresas (Oficial o Jefe de Seguridad de la Información, Gerente o persona designada), el Instituto de Auditores Internos (IAI) menciona: “La actividad de Auditoría Interna debe evaluar la eficacia y contribuir a la mejora de los procesos de gestión de riesgos.”. (pág. 178)

2.2.10. Ciberseguridad

(ISACA, 2013) hace referencia sobre estudios de Ciberseguridad:

> ¿Qué es la Ciberseguridad?
>
> Las palabras Ciberseguridad, cibercrimen y ciberguerra han tomado relevancia en el mundo de la seguridad en general. Esto es debido, en parte, a la evolución tecnológica y, en mayor medida, al incremento en las violaciones de seguridad, actos criminales y a la presencia de armas de guerra basadas en la información. En esta publicación, los incidentes de Ciberseguridad, crímenes o actos de guerra son tratados simplemente como actos humanos u omisiones. Los mitos y supersticiones del pasado ejemplarizados por alguna literatura de los años 90 se han mostrado que son infundados, transformando la Ciberseguridad en un trabajo de gestión como cualquier otra actividad de seguridad.

> El término “ciber” desde el punto de vista de la seguridad de la información requiere de una explicación, pues es usado de forma amplia y, a menudo, malentendido. Para los propósitos de esta publicación, la Ciberseguridad acompaña a todas las medidas de protección empresarial e individual frente a ataques intencionados, violaciones de seguridad e incidentes, así como de sus consecuencias. En la práctica, la Ciberseguridad se encarga principalmente de aquellos tipos de ataque, violaciones de seguridad o incidentes dirigidos, sofisticados y difíciles de detectar o gestionar. El amplio campo de los ataques y delitos oportunistas pueden ser tratados empleando estrategias y herramientas simples a la par que efectivas. Como resultado, el foco de la Ciberseguridad está puesto sobre lo que conoce como amenazas persistentes avanzadas (APTs), la ciberguerra y su impacto sobre empresas e individuos.
>
> Independientemente de la generalización del término, la Ciberseguridad debería estar alineada con el resto de puntos que involucra la gestión integral de la seguridad. Esto incluye la gobernanza, la gestión y el aseguramiento. En este sentido, la noción general de la seguridad es sistémica en lugar de lineal, reconociendo la idea del estar seguro como un estado transitorio que requiere un mantenimiento y una mejora continua para conocer las necesidades y requisitos de las partes interesadas. (ISACA, 2013)

En un publicación de la revista ISACA Journal el autor del artículo “El papel de la tecnología en la gestión del riesgo empresarial”, Bayuk (2018) hace mención: “Las amenazas de ciberseguridad y otras preocupaciones tecnológicas disruptivas están entre lo más importante para los miembros de la alta gerencia de hoy”. (pág. 17)

En otra publicación de la revista ISACA Journal el autor del artículo “Construyendo puentes con el directorio - innovación en la gobernanza de la información”, Sean (2018) manifiesta, “(…) La seguridad de los datos es ahora un esfuerzo de toda la empresa y una gran preocupación para los directorios y altos ejecutivos. A nivel mundial, existen docenas de leyes que regulan cómo las empresas administran la ciberseguridad y qué deben hacer en caso de una violación de datos (…). (pág. 35)

También hace mención Sean (2018)

> (…) La mayoría de las organizaciones almacena datos no estructurados que incluyen datos confidenciales o PII (información de identificación personal) que pueden estar sujetos a leyes de privacidad. Tomarse el tiempo para escanear archivos compartidos para datos confidenciales, identificar información crítica y obtenerla bajo llave puede ayudar a mitigar el riesgo de pérdida de propiedad intelectual y secretos comerciales, y el riesgo operativo y de reputación relacionado con la administración de una violación de datos (…). (Sean, 2018, pág. 36)

En este punto existe una concordancia en el punto de esclarecer que efectivamente las empresas están sujetas a diversas normas o regulaciones, dado por un entorno tecnológico cambiante, en ocasiones por desconocimiento de la seguridad, donde la administración del riesgo de negocio es prioritaria para el cumplimiento legal y seguir operando en el país.

En la publicación de Steve Piper toma en referencia lo siguiente:

"La piratería se ha transformado ahora en una industria que mueve miles de millones de dólares. Atrás quedaron los días de la piratería por pura diversión.". (Piper, 2013, pág. 12)

Piper (2013) toma en referencia lo siguiente sobre los ciberdelincuentes: "Dicho de manera simple, los ciberdelincuentes son personas que cometen acciones de piratería informática para obtener un beneficio económico. En la mayoría de los casos, penetran en las redes de las empresas con el fin de robar (…)" (pág. 12)

En la publicación de ISACA (2013) "Transformando la Ciberseguridad", hace referencia: "Desde una perspectiva de la ciberseguridad, las amenazas y vulnerabilidades necesitan ser categorizadas, así como, el riesgo asociado. Al contrario que en la seguridad de la información en general, el foco se encuentra en las amenazas avanzadas y sobre las vulnerabilidades que no pueden ser, ni fácilmente detectables, ni solventadas". (pág. 31)

En la publicación de E&Y (2018) comenta: "Las organizaciones deben enfocarse en la seguridad de TI y la seguridad de la información para evitar ser víctimas de ciberamenazas mediante el desarrollo de un programa cibernético de auditoría (…)". (pág. 29)

2.2.11. Ley de Protección de Datos Personales N° 29733 (LPDP)

Actualmente todas las empresas tanto privadas o públicas se encuentran obligadas a cumplir con esta ley para ello se cita del artículo 1 el siguiente texto:

"La presente Ley tiene el objeto de garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen". (Congreso de la República del Perú, 2011)

La Ley de Protección de Datos Personales estable como faltas "La Autoridad Nacional de Protección de Datos Personales determina la infracción cometida y el monto de la multa imponible mediante resolución debidamente motivada. Para la graduación del monto de las multas, se toman en cuenta los criterios establecidos en el artículo 230, numeral 3), de la Ley 27444, Ley del Procedimiento Administrativo General, o la que haga sus veces". (Congreso de la República del Perú, 2011)

Sobre esta ley es necesario citar en un artículo publicado por el Ing. CIP Edward Zárate Carlos comenta:

> Como puede verse debe ser preocupación de las empresas reforzar los derechos de las personas de modo que la entrega y usos de los datos personales tengan la garantía de una buena administración. Las empresas asimismo requieren elevar los niveles de protección de datos y seguridad de la información que son administrados cotidianamente. Una forma es efectuar un diagnóstico de la brecha entre la forma de los datos obtenidos para racionalizar la administración de la minería de datos, estas acciones pueden sistematizarse mediante software sobre monitorización y filtros de la protección de datos.

Debe tenerse en cuenta que, de acuerdo a lo dispuesto por la Primera Disposición Complementaria Transitoria el 08 de mayo de 2015 venció el plazo para que los bancos de datos personales existentes deban adecuarse a lo establecido por la normativa. (Zárate Carlos, 2017)

E&Y, 2018 menciona:

> La LPDP exige que la organización sea capaz de demostrar que cumple los requisitos de forma efectiva. Adoptar una estructura basada en controles

internos que abarque las tres líneas de defensa de una organización brindará en enfoque disciplinado e integral para abordar el riesgo de privacidad y el cumplimiento. (Ernst & Young, 2018, pág. 43)

2.2.12. Directiva de Seguridad de la Ley de Protección de Datos

La Directiva de Seguridad de la Ley de Protección de Datos tiene por finalidad facilitar la adecuación de la ley, por tanto establece "Garantizar la seguridad de los datos personales contenidos o destinados a ser contenidos en bancos de datos personales, mediante medidas de seguridad que protejan a los bancos de datos personales, de conformidad con la Ley Nº 29733 y su reglamento". (Ministerio de Justicia y Derechos Humanos, 2013, pág. 9)

Además, "Con la expedición de la Ley Nº 29733 – Ley de Protección de Datos Personales y de su respectivo Reglamento, aprobado con Decreto Supremo Nº 003-2013-JUS, el Perú cuenta ya con un marco jurídico para garantizar el respeto al derecho fundamental a la protección de datos personales (…).". (Ministerio de Justicia y Derechos Humanos, 2013, pág. 4)

Este documento es un facilitador para la adecuación de las normas de seguridad aplicables para las diversas empresas (pequeñas, medianas y grandes) de cara al cumplimiento de la Ley de Protección de Datos Personales.

2.2.13. Aspectos legales para la Protección del Secreto de las Telecomunicaciones

Las empresas del sector Telecomunicaciones para ejercer sus funciones y responsabilidades dentro del país tienen la obligación de cumplir con ciertas Leyes, normas y disposiciones legales.

Este punto es uno de los factores que propician la base y establece las reglas para las empresas de este sector, en función a su cumplimiento y ejecución, tomando un enfoque de riesgos, donde se aborda las prácticas de privacidad, políticas que impactan a la seguridad informática, los procesos de gestión y operación, protección de datos; con la finalidad que sean evaluados constantemente.

A continuación se detallan las principales Leyes y Normas aplicables para las empresas del sector Telecomunicaciones:

1. En la Constitución Política

En su **"**Artículo 2°.- Toda persona tiene derecho (…)

6. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar". (Congreso Constituyente Democrático, 1993)

También, hace mención "10. Las comunicaciones, telecomunicaciones o sus instrumentos sólo pueden ser abiertos, incautados, interceptados o intervenidos por mandamiento motivado del juez, con las garantías previstas en la ley. Se guarda secreto de los asuntos ajenos al hecho que motiva su examen (…)" (Congreso Constituyente Democrático, 1993)

2. Artículos 161° y 162° del Código Penal

En el capítulo IV, del Código Penal se hace referencia con respecto a la violación del secreto de las comunicaciones

Violación de correspondencia

"Artículo 161°.- El que abre, indebidamente, una carta, un pliego, telegrama, radiograma, despacho telefónico u otro documento de naturaleza análoga, que no le esté dirigido, o se apodera indebidamente de alguno de estos documentos, aunque no esté cerrado, será reprimido con pena privativa de libertad no mayor de dos años y con sesenta a noventa días-multa". (Ministerio de Justicia y Derechos Humanos, 2016, pág. 96)

Artículo 162°.- Interferencia telefónica

"El que, indebidamente, interviene o interfiere o escucha una conversación telefónica o similar, será reprimido con pena privativa de libertad no menor de cinco ni mayor de diez años (…)." (Ministerio de Justicia y Derechos Humanos, 2016, pág. 96)

3. Ley de Telecomunicaciones

Texto único aprobado de la Ley de Telecomunicaciones aprobado por Decreto Supremo 013-093-TCC.

"Artículo 4.- Toda persona tiene derecho a la inviolabilidad y al secreto de las telecomunicaciones. El Ministerio de Transportes,

Comunicaciones, Vivienda y Construcción se encarga de proteger este derecho". (Ministerio de Justicia, 1993)

"Artículo 87.- Constituyen infracciones muy graves: (…)

4). La interceptación o interferencia no autorizadas de los servicios de telecomunicaciones no destinados al uso libre del público en general". (Ministerio de Justicia, 1993)

"(…) La divulgación de la existencia o del contenido, o la publicación o cualquier otro uso de toda clase de información obtenida mediante la interceptación o interferencia de los servicios de telecomunicaciones no destinados al uso público general (…)". (Ministerio de Justicia, 1993)

4. Ley 27697 - Ley que otorga facultad al Fiscal para la intervención y control de comunicaciones y documentos privados en Caso Excepcional

Dicho brevemente, esta Ley tiene "(…) por finalidad desarrollar legislativamente la facultad constitucional dada a los jueces para conocer y controlar las comunicaciones de las personas que son materia de investigación preliminar o jurisdiccional." (Congreso del Perú, 2002)

Esta ley permite a los jueces levantar el Secreto de las Telecomunicaciones por citar algunos casos como: Secuestro agravado, tráfico de menores, tráfico ilícito de drogas, corrupción de funcionarios, entre otros.

5. Reglamento General del Secreto de las Telecomunicaciones

Según el DECRETO SUPREMO Nº 020-2007-MTC establece en el artículo 13, que toma en consideración la inviolabilidad y secreto de las telecomunicaciones, se indica, "(…) cuando deliberadamente una persona que no es quien origina ni es el destinatario de la comunicación, sustrae, intercepta, interfiere, cambia o altera su texto, desvía su curso, publica, divulga, utiliza, trata de conocer o facilitar que él mismo u otra persona, conozca la existencia o el contenido de cualquier comunicación (…).". (Ministerio de Justicia, 2007)

Además en el artículo 258, sobre las infracciones muy graves, constituye dentro de sus faltas: "(...) El incumplimiento de las obligaciones de los operadores de servicios públicos de telecomunicaciones para salvaguardar la inviolabilidad y el secreto de las telecomunicaciones, así como la

protección de datos personales, conforme a la normativa que regulan estas obligaciones." (Ministerio de Justicia, 2007)

6. **Resolución Ministerial N°111 – 2009 - MTC/03**

"Norma que establece medidas destinadas a salvaguardar a la inviolabilidad y el secreto de las telecomunicaciones y protección de datos personales y regula las acciones de supervisión y control a cargo del Ministerio de Transportes y Comunicaciones". (Ministerio de Transportes y Comunicaciones, 2009)

7. **De las obligaciones de los operadores de Telecomunicaciones relativa a la inviolabilidad y al Secreto de las Telecomunicaciones y la Protección de datos personales.**

Dentro de las obligaciones se establece:

"10.3 Los Operadores de Telecomunicaciones tienen la obligación de respetar y salvaguardar el secreto de las telecomunicaciones y proteger los datos personales de sus Abonados y/o Usuarios, salvo las excepciones previstas en la legislación vigente (…)". (Ministerio de Transportes y Comunicaciones, 2009)

Además en el punto 10.4 se refuerza la responsabilidad de cumplir con varias medidas (accesos), procedimientos que deben tener implementados, además añade "(…) sólo el personal debidamente autorizado, propio de terceros, acceda a locales y sistemas como acceso restringido, los que serán previamente determinados por el Operador de Telecomunicaciones, en función a su red, tanto en planta interna como externa (…)". (Ministerio de Transportes y Comunicaciones, 2009)

En resumen, esta Norma precisa sobre la información que debe ser presentada, el régimen de las visitas e inspecciones, y las consecuencias por incumplimiento o infracción.

7. Ley de Delitos Informáticos N° 30096

En la Ley 30096, se establece en resumen en su artículo 7, sobre la interceptación de datos informáticos, es decir aquel que intercepta transmisiones privadas a través de un sistema informático, podrá pugnar condena entre 3 y 6 años. (Congreso de la República del Perú, 2013)

De igual manera, esta ley fue modificada por la Ley 30171 en el año 2014, que permite una interpretación más concreta sobre los delitos informáticos, se toma como excepción los casos de hacking ético, en la publicación del Dr. Julio Núñez, hace una precisión más completa sobre la modificación de esta ley. (Núñez Ponce, 2014)

8. **Ley de Desarrollo de las Funciones y Facultades del Organismo Supervisor de Inversión Privada en Telecomunicaciones - OSIPTEL**

"Artículo 8.- Secreto e inviolabilidad de las comunicaciones

8.1 En ningún caso la autoridad competente puede solicitar información que signifique la violación del derecho al secreto y la inviolabilidad de las comunicaciones, a que se refiere el inciso 10) del Artículo 2 de la Constitución Política del Perú". (Congreso de la República, 2000)

2.3. Marcos Conceptuales

En este glosario de términos de uso frecuente en la Gestión de Riesgos de Seguridad de la Información. En la elaboración del glosario se ha tenido en consideración las definiciones recogidas en los principales estándares y autores que se detallan en el apartado. Para cada término se ha seleccionado, lo más adecuado en el contexto de la investigación.

1. **Activo**

   "Algo de valor ya sea tangible o intangible dignos de protección, incluidas las personas, la información, la infraestructura, las finanzas y la reputación". (ISACA, 2009)

2. **Análisis del riesgo**

   "Proceso que permite comprender la naturaleza del riesgo y determinar el nivel de riesgo". (Norma Técnica Peruana NTP-ISO/IEC 31000:2011, 2011 Revisada 2016)

3. **Amenaza**

   "Cualquier circunstancia o evento que pueda explotar una vulnerabilidad específica de un sistema de información y comunicaciones, resultando en una pérdida de confidencialidad, integridad, disponibilidad, autenticidad o

trazabilidad de la información manejada o de la integridad o disponibilidad del propio sistema". (Merino Bada & Cañizares Sales, 2011)

4. **Apetito de riesgo**

   La cantidad de riesgo, en un nivel más amplio, que la entidad está dispuesta a aceptar en el cumplimiento de su misión. (ISACA, 2009)

5. **COBIT**

   Conocido como Objetivos de Control para Tecnologías de Información o Relacionadas (COBIT). Además "COBIT describe cinco principios y siete facilitadores que dan soporte a las empresas en el desarrollo, implementación y mejora continua y supervisión de buenas prácticas relacionadas con el gobierno y la gestión de TI". (ISACA, 2012).

6. **Confidencialidad**

   "Es la garantía de que la información no es conocida por personas, organizaciones o procesos que no disponen de la autorización necesaria". (Merino Bada & Cañizares Sales, 2011)

7. **Disponibilidad**

   "Es la garantía que de la información es accesible en el momento de que los usuarios autorizados (personas, organizaciones, procesos) tienen la necesidad de acceder a ella". (Merino Bada & Cañizares Sales, 2011)

8. **Gestión del riesgo**

   "Actividades coordinadas para dirigir y controlar una organización en lo relativo al riesgo". (Norma Técnica Peruana NTP-ISO/IEC 31000:2011, 2011 Revisada 2016)

9. **Evaluación del riesgo**

   "Proceso de comparación de los resultados del análisis del riesgo con los criterios de riesgo para determinar si el riesgo y/o su magnitud son aceptables o tolerables". (Norma Técnica Peruana NTP-ISO/IEC 31000:2011, 2011 Revisada 2016)

10. **IAI**

    Instituto de Auditores Internos.

11. **Identificación del riesgo**

    "Proceso de búsqueda, reconocimiento y descripción de riesgos". (Norma Técnica Peruana NTP-ISO/IEC 31000:2011, 2011 Revisada 2016)

12. **Incidente**

    Es un evento o una serie de eventos no deseados que tienen una probabilidad significativa de comprometer operaciones del negocio y amenazar la seguridad de la información.

13. **Integridad**

    "Es la garantía de que la información no ha sido transferida, ni modificada de forma no autorizada durante su procesamiento, transporte o almacenamiento, y que además permite detectar las posibles modificaciones que pudieran haberse producido". (Merino Bada & Cañizares Sales, 2011)

14. **ISACA**

    Information Systems Audit and Control Association (Asociación de Auditoría y Control de Sistemas de Información).

    Ayuda a los profesionales globales a liderar, adaptar y asegurar la confianza en un mundo digital en evolución ofreciendo conocimiento, estándares, relaciones, acreditación y desarrollo de carrera innovadores y de primera clase. Establecida en 1969, ISACA es una asociación global sin ánimo de lucro de 140 000 profesionales en 180 países. ISACA también ofrece Cybersecurity Nexus™ (CSX), un recurso integral y global en Ciberseguridad, y COBIT®, un marco de negocio para gobernar la tecnología de la empresa. ISACA adicionalmente promueve el avance y certificación de habilidades y conocimientos críticos para el negocio, a través de las certificaciones globalmente respetadas: Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) y Certified in Risk and Information Systems Control™ (CRISC™). La asociación tiene más de 200 capítulos en todo el mundo. (ISACA, 2018)

15. **ISO/IEC**

    Organización Internacional de Normalización - Comisión Electrotécnica Internacional.

16. **LPDP**

    Ley de Protección de Datos Personales.

17. **NTP**

    Norma Técnica Peruana.

18. **OCDE**

Organización para la Cooperación y el Desarrollo Económicos.

19. **PTR**

    Plan de Tratamiento de Riesgos.

20. **Proceso de gestión de riesgos**

    "Aplicación sistemática de políticas de gestión, procedimientos y prácticas a las actividades de comunicación, consulta, establecimiento del contexto e identificación, análisis, evaluación, tratamiento, seguimiento y revisión del riesgo". (ISO/IEC 27000:2018, 2018)

21. **Probabilidad**

    "Posibilidad de que algún hecho se produzca". (Norma Técnica Peruana NTP-ISO/IEC 31000:2011, 2011 Revisada 2016)

22. **Riesgo**

    "Efecto de la incertidumbre sobre los objetivos". (Norma Técnica Peruana NTP-ISO/IEC 31000:2011, 2011 Revisada 2016)

23. **Riesgo residual**

    Nivel restante de riesgo después de que se han tomado medidas de tratamiento del riesgo. (ISO/IEC 27000:2018, 2018)

24. **Seguridad de la información**

    Corresponde a salvaguardar la confidencialidad, integridad y disponibilidad de la información.

25. **SGSI**

    Sistema de Gestión de Seguridad de la Información.

26. **TIC**

    Tecnologías de la Información y la Comunicación.

27. **Tolerancia de riesgo**

    "El nivel aceptable de variación de que la administración está dispuesta a permitir un riesgo particular, ya que persigue objetivos". (ISACA, 2009)

28. **Tratamiento del riesgo**

    "Proceso destinado a modificar el riesgo". (Norma Técnica Peruana NTP-ISO/IEC 31000:2011, 2011 Revisada 2016).

29. **Vulnerabilidad**

    "Debilidad de un activo o control que puede ser explotado por una o más amenazas". (ISO/IEC 27000:2018, 2018)

Capítulo 3 – METODOLOGÍA

En el presente capítulo se va especificar la metodología que fue empleada para obtener la información necesaria para la elaboración de la presente tesis.

3.1. Tipo y Diseño de Investigación

Para realizar el presente tesis se seleccionó el tipo de investigación no experimental.

En el diseño de la investigación se ha considerado una investigación descriptiva que formula una hipótesis para pronosticar un hecho, se analiza la relación existente sobre un conjunto de variables para determinar si la hipótesis es válida.

La investigación no experimental, según Hernández, Fernández & Baptista (2014) "es la que se realiza sin manipular deliberadamente las variables independientes; se basa en categorías, conceptos, variables, sucesos, fenómenos o contextos que ya ocurrieron o se dieron sin la intervención directa del investigador". (pág. 152)

Diseños transeccionales descriptivos

Según Hernández, Fernández & Baptista (2014), en su publicación menciona "Los diseños transeccionales descriptivos tienen como objetivo indagar la incidencia de las modalidades o niveles de una o más variables en una población. El procedimiento consiste en ubicar en una o diversas variables a un grupo de personas u otros seres vivos, objetos, situaciones, contextos, fenómenos, comunidades, etc., y proporcionar su descripción". (pág. 155)

Cuadro 1 Correspondencia entre tipos de estudio, hipótesis y diseño de investigación

Estudio	Hipótesis	Posibles diseños
Exploratorio	• No se establecen, lo que se puede formular son conjeturas iniciales	• Transeccional exploratorio o descriptivo • Preexperimental
Descriptivo	• Descriptiva	• Preexperimental • Transeccional descriptivo
Correlacional	• Diferencia de grupos sin atribuir causalidad	• Cuasiexperimental • Transeccional correlacional • Longitudinal (no experimental)
	• Correlacional	• Cuasiexperimental • Transeccional correlacional • Longitudinal (no experimental)
Explicativo	• Diferencia de grupos atribuyendo causalidad	• Experimental puro • Cuasiexperimental, longitudinal y transeccional causal (cuando hay bases para inferir causalidad, un mínimo de control y análisis estadísticos apropiados para relaciones causales)
	• Causales	• Experimental puro • Cuasiexperimental, longitudinal y transeccional causal (cuando hay bases para inferir causalidad, un mínimo de control y análisis estadísticos apropiados para relaciones causales)

Fuente. (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2014)

3.2. Unidad de análisis

Para esta tesis, se abordó como muestra a los colaboradores de las empresas de Telecomunicaciones que cuentan con más de 5000 colaboradores, perteneciente a la ciudad de Lima – Metropolitana.

Cuadro 2 Cuadro de cargo de colaboradores

Ítem	Cargo	Cantidad
1	Gerencia	20
2	Jefes	30
4	Coordinadores	18
5	Analistas	36
	TOTAL	**104**

Fuente. Elaboración propia

3.3. Población de estudio

La población de la tesis de estudio fue 104 personas, perteneciente al sector Telecomunicaciones ubicada en la ciudad de Lima Metropolitana.

La información de las empresas operadoras de Telecomunicaciones se obtuvo desde el Portal OSIPTEL, en el siguiente cuadro se apreciar el detalle:

Cuadro 3 Empresas Operadoras de Telecomunicaciones en el Perú

Empresas operadoras		
Americatel Perú S.A.	0800 - 70099	http://www.americatel.com.pe
Bitel	0800 - 79123	http://www.bitel.com.pe/
Claro	Desde sus Teléfonos: 123	http://www.claro.com.pe/
Convergia Perú S.A.	01 - 640 1010	http://www.convergia.com.pe/
Entel Perú	0800 - 18844 / 0800 - 11236 (Desde provincias)	http://www.entel.pe
Gilat to Home	0800 - 70700	http://www.gilat.com.pe/
IDT Perú	1914 - 104	http://www.1914.com.pe
Impsat Perú (Level 3)	01 - 705 5667	http://www.level3.com/es/
Infoductos y Telecomunicaciones del Perú S.A.	0800 - 119 01	http://www.infoductos.com.pe/
Optical Technologies S.A.C.	01 - 500 3400	http://www.optical.pe
Rural Telecom	Desde sus Teléfonos Públicos: 104	http://www.ruraltelecom.com.pe
Telefónica Móviles S.A.	Desde sus Teléfonos: 123 790 - 0123	http://www.movistar.com.pe
Telefónica del Perú S.A.A.	Desde sus Teléfonos: 104	http://www.telefonica.com.pe

Fuente: OSIPTEL (Organismo Supervisor de Inversión Privada en Telecomunicaciones, 2018)

3.4. Tamaño de muestra

Según Hernández, Fernández & Baptista (2014) menciona:

> "Cuando se elabora una muestra probabilística, uno debe preguntarse: dado que una población es de N (tamaño de muestra), ¿cuál es el menor número de unidades muestrales (personas, casos, organizaciones, capítulos de telenovelas, etc.) que necesito para conformar una muestra (n) que me asegure un determinado nivel de error estándar, digamos menor de 0.01?" (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2014, pág. 178)

> Además añade: “La respuesta consiste en encontrar una muestra que sea representativa del universo o población con cierta posibilidad de error (se pretende minimizar) y nivel de confianza (maximizar), así como probabilidad”. (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2014, pág. 178)

A continuación de detalla el cálculo de la muestra:

$$\frac{k^2 N p q}{e^2(N-1) + k^2 p q}$$

N: Tamaño de la población o universo (104 personas).

k: Constante que depende del nivel de confianza que asignemos (95%).

p: Proporción de personas de estudio.

q: Proporción de personas que no tienen una misma característica, es decir, es 1-p.

e: Error muestral esperado (5%).

Resultado: 82 personas.

3.5. Selección de muestra

La selección de la muestra se realizó en función a la factibilidad en el acceso a los procesos de negocio y disponibilidad de los colaboradores.

Según Hernández, Fernández & Baptista (2014) menciona, “Aquí el procedimiento no es mecánico ni se basa en fórmulas de probabilidad, sino que depende del proceso de toma de decisiones de un investigador o de un grupo de investigadores y, desde luego, las muestras seleccionadas obedecen a otros criterios de investigación (…)”. (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2014, pág. 176)

Cuadro 4 Selección de muestra

Ítem	Cargo/ Jerarquía	Total población	Muestra
1	Gerencia	20	11
2	Jefes	30	25
4	Coordinadores	18	15
5	Analistas	36	31
		N= 104	n= 82

Fuente. Elaboración propia

3.5.1. Muestreo de participantes voluntarios

En estos casos, la elección de los participantes depende de circunstancias muy variadas. A esta clase de muestra también se le puede llamar autoseleccionada, ya que las personas se proponen como participantes en el estudio o responden a una invitación. (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2014)

3.6. Técnicas de recolección de datos

Según Hernández, Fernández & Baptista (2014) menciona "Generalmente utilizan cuestionarios que se aplican en diferentes contextos (entrevistas en persona, por medios electrónicos como correos o páginas web, en grupo, etc.)". (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2014, pág. 159)

Para el caso de la presente tesis, se tomó la encuesta.

3.6.1. La encuesta

Para la presente tesis, se utilizó los servicios web para realizar las encuestas y recolección de datos.

Las técnicas de recolección de datos, mencionadas anteriormente, nos permitieron obtener información detallada que luego fueron analizadas e interpretadas.

3.7. Modelo de encuesta

Previamente, para realizar la encuesta se realizó la validación de la encuesta por juicios de expertos. Luego, se ejecutó la encuesta con la finalidad de

extraer información relevante, analizar los resultados obtenidos y proceder a generar métricas de gestión.

Véase en el Anexos 9.4, páginas 112-114.

Dicho lo anterior, es necesario precisar que la encuesta contó con la validación de opinión de expertos.

Véase en el Anexo 9.5, página 115.

3.8. Modelo de instrumento y matriz de operacionalización

La Matriz Operacionalización permite elaborar en base a una estructura, los problemas, objetivos e hipótesis. Además, permite validar los elementos claves del inicio de la investigación científica, la interrelación entre las variables, la conexión lógica desde el título, los problemas, los objetivos e hipótesis.

Véase Capítulo de Anexos 9.6, página 116.

Capítulo 4 - RESULTADOS Y DISCUSIÓN

En este capítulo de la tesis se muestra los resultados obtenidos y se hace un análisis del mismo.

4.1. Análisis e interpretación de la información

Según Hernández, Fernández & Baptista (2014) menciona "se revisan los hallazgos más importantes y se incluyen los puntos de vista y las reflexiones de los participantes y del investigador respecto al significado de los datos, los resultados y el estudio en general; además de evidenciar las limitaciones de la investigación y hacer sugerencias para futuras indagaciones". (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2014, pág. 510)

Las herramientas informáticas que nos brindó soporte fue Microsoft Excel para apoyo en la muestra de resultados.

A continuación se presenta los resultados obtenidos, consta de diez (10) preguntas:

1. **De manera general ¿Tiene conocimiento de la difusión y publicación de políticas o normativas de Seguridad de la Información/ Gestión de Riesgos?**

Cuadro 5 Encuesta pregunta 1

Opciones de respuesta	Porcentaje
Si	57.3%
No	30.5%
Desconozco	12.2%

Fuente. Elaboración propia

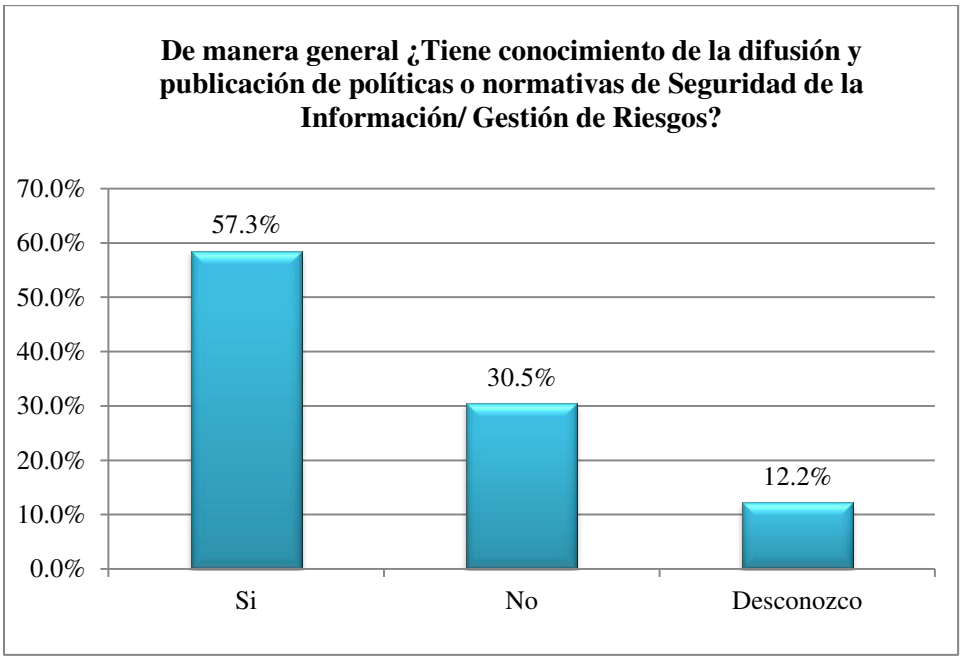


Figura 4: De manera general ¿Tiene conocimiento de la difusión y publicación de políticas o normativas de Seguridad de la Información/ Gestión de Riesgos?

Fuente. Elaboración propia

Interpretación:

Según los resultados obtenidos se puede identificar que solo un poco más de la mitad de los encuestados conoce sobre la difusión y publicación de documentos normativos, mientras que un alarmante 30.5% no conoce la existencia de este tipo de documentos mientras que el grupo restante desconoce o no tiene conocimiento, es por ello que las organizaciones deben tomar foco en la concientización y tomar el liderazgo de los riesgos identificados.

2. **En general ¿Cuáles son los riesgos qué se expone la organización en la inapropiada gestión de riesgos de seguridad de la información?**

Cuadro 6 Encuesta pregunta 2

Opciones de Respuesta	**Porcentaje de Respuestas**
Fuga de información	46.3%
Acceso de personal no autorizado	19.5%
Fraudes	19.5%
Pérdida de la auditabilidad de la gestión	12.2%
Otros	2.4%

Fuente. Elaboración propia

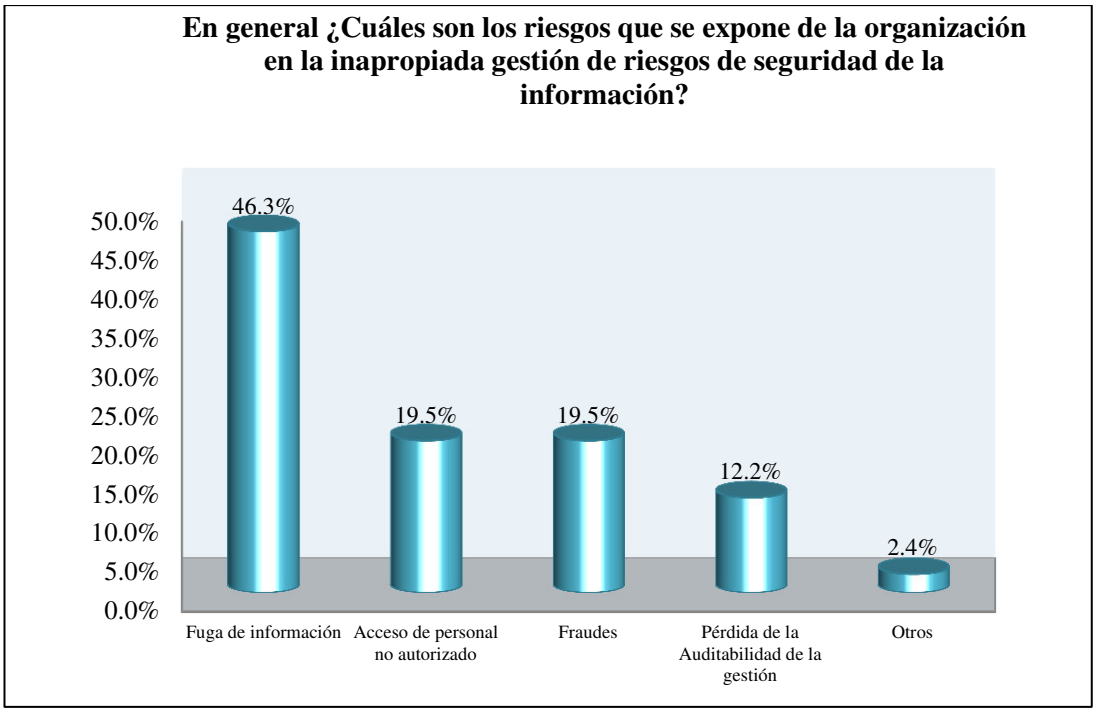


Figura 5: En general ¿Cuáles son los riesgos qué se expone de la organización en la inapropiada gestión de accesos?

Fuente. Elaboración propia

Cuadro 7 Estadísticas

Estadísticas				
Mínimo	**Máximo**	**Mediana**	**Media**	**Desviación estándar**
1,00	5,00	2,00	2,05	1,17

Fuente. Elaboración propia

Interpretación:

Se puede apreciar según la encuesta realizada que claramente la fuga de información es el riesgo más importante con un casi 50% que afronta las organizaciones en la inadecuada gestión de accesos, mientras que el acceso de personal no autorizado y fraudes se puede considerar un empate técnico y la falta de trazabilidad representa un riesgo menor con 12.2% (perfilamiento indebido, falta de monitoreo, otros).

Para mitigar los riesgos identificados se recomienda:

- Segregación de funciones.
- Revisión de derechos de accesos.
- Implementar un procedimiento de gestión de accesos.

3. **¿Cuál de las siguientes tecnologías considera como la mayor preocupación de fuga de información?**

Cuadro 8 Encuesta pregunta 3

Opciones de Respuesta	Porcentaje de Respuesta
Medios extraíbles (USB, discos duros)	51.2%
Equipos móviles	26.8%
Servicios en la nube	13.4%
Software de control de escritorio	7.3%
Otro	1.2%

Fuente. Elaboración propia

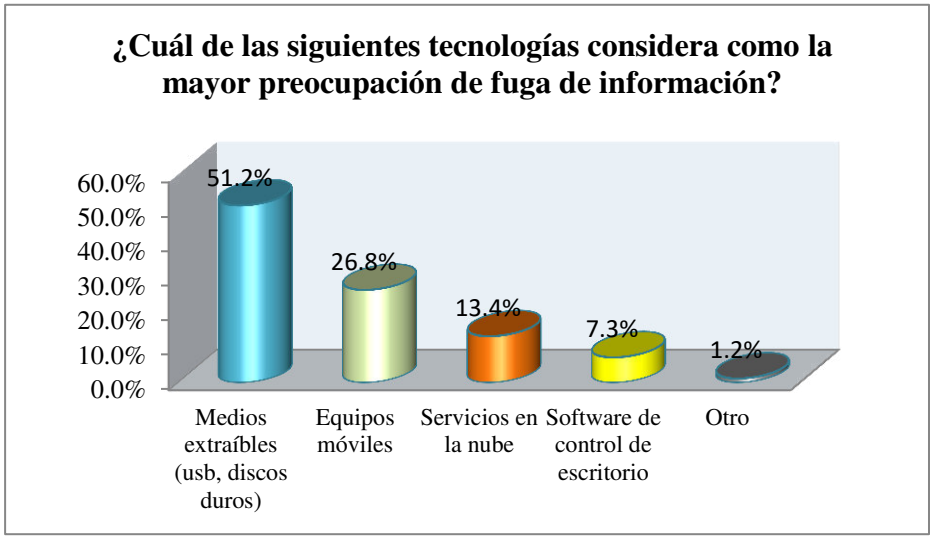


Figura 6: ¿Cuál de las siguientes tecnologías considera como la mayor preocupación de fuga de información?

Fuente. Elaboración propia

Cuadro 9 Estadísticas

Estadísticas				
Mínimo	**Máximo**	**Mediana**	**Media**	**Desviación estándar**
1,00	5,00	1,00	1,80	1,01

Fuente. Elaboración propia

Comentario:

Se puede apreciar que, más de la mitad de los encuestados considera que la mayor preocupación en la fuga de información es el uso de medio de extraíbles con un 51.2%, en el cual podría existir serios impactos legales y regulatorios, en segundo lugar se muestra el uso de equipos móviles debido

que estos aparatos cuentan con medio de grabación, fotografía y almacenamiento de información, luego se aprecia el uso de los servicios en la nube que es una tecnología que está en crecimiento debido que no necesita medios físicos para guardar o extrae información, luego se muestra al uso de software de control de escritorio cual permite acceder a otras estaciones de trabajo con la finalidad de extraer, eliminar o modificar información y por último el 1.2% considera que por otros medios se puede extraer información (uso de servidores de transferencia ,correo electrónico).

4. **En general ¿Tiene conocimiento de la Ley de Protección de Datos Personales Nº 29733?**

Cuadro 10 Encuesta pregunta 4

Opciones de Respuesta	**Porcentaje de Respuesta**
Si	42.7%
No	51.2%
Desconozco	6.1%

Fuente. Elaboración propia

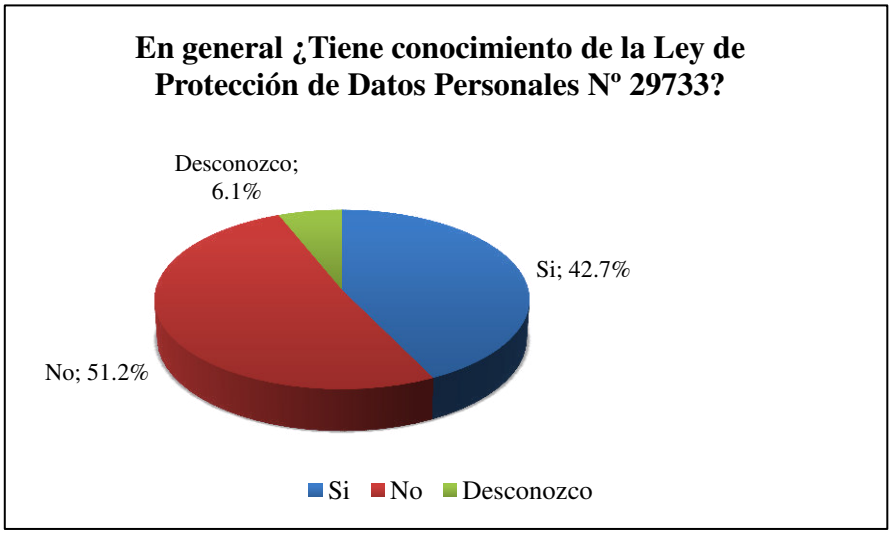


Figura 7: ¿Tiene conocimiento de la Ley de Protección de Datos Personales?

Fuente. Elaboración propia

Interpretación:

Es importante mencionar, que más del 50% de los encuestados no tiene conocimiento de la Ley de Protección de Datos Personales Nº 29733 y sus implicancias en la salvaguarda de la información privada de los usuarios, el cual rige desde mayo del 2015, tanto las empresas privadas o públicas se encuentran obligadas a implementar los lineamientos de esta ley, mientras un 42.7% conoce los lineamientos de la ley en mención.

5. **¿Se ha tenido en cuenta la seguridad de la información como criterio en las fases de desarrollo y puesta en producción de las aplicaciones usadas en los proyectos?**

Cuadro 11 Encuesta pregunta 5

Opciones de Respuesta	Porcentaje de Respuesta
Si	24.4%
No	19.5%
A veces	35.4%
Desconozco	20.7%

Fuente. Elaboración propia

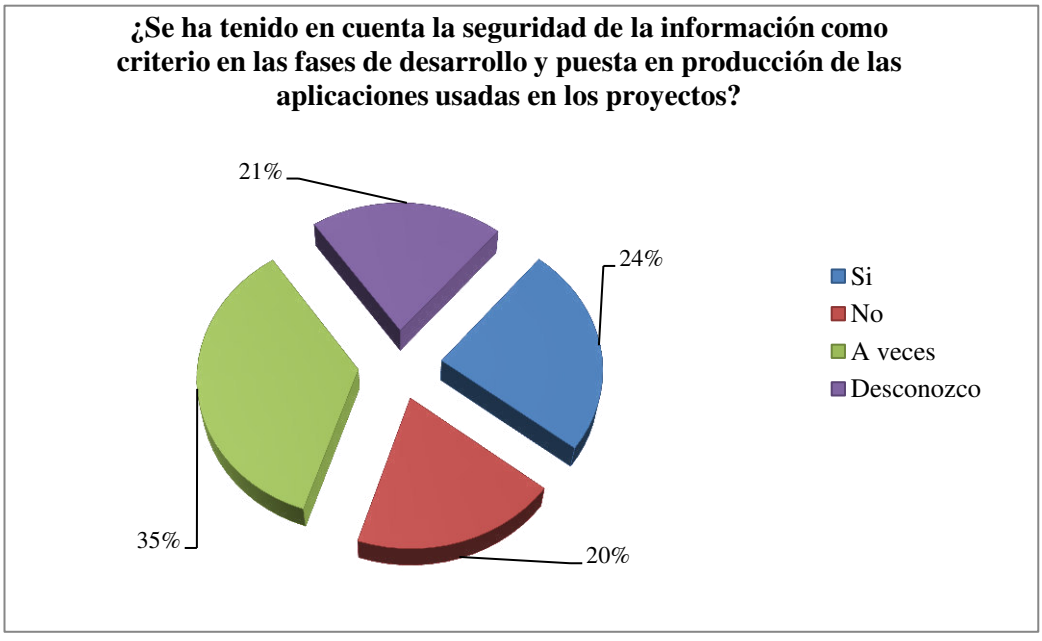


Figura 8: ¿Se ha tenido en cuenta la seguridad de la información como criterio en las fases de desarrollo y puesta en producción de las aplicaciones usadas en los proyectos?

Fuente. Elaboración propia

Interpretación:

Solo un tercio de encuestados indica que los proyectos está considerada la seguridad de la información como parte de los entregables estipulados tanto en los contratos y en la operación del servicio, un 20% considera que no es necesaria esta solicitud obviando los riesgos que se expone, un 35% de los encuestados que representa la mayor cantidad de encuestados indica que solo en algunos proyectos según la criticidad del proyecto incluye a la seguridad de la información, mientras que el 20.7% desconoce este punto por la falta de conocimiento o no estar inmerso en la gestión de proyectos.

6. **En general ¿Se ha visto afectado durante el presente año por incidentes de seguridad de la información? (5 representa muy importante y 1 nada importante).**

Cuadro 12 Encuesta pregunta 6

Opciones de Respuesta	**Nada importante**	**Poco moderado**	**Moderado**	**Importante**	**Muy importante**
Modificación o eliminación de información	31.71 %	26.83 %	24.39 %	8.54 %	8.54 %
Carpetas compartidas con acceso a "todos"	21.95 %	28.05 %	21.95 %	13.41 %	14.63 %
Instalación de software no autorizado	24.39 %	17.07 %	24.39 %	20.73 %	13.41 %
Infección de virus	13.41 %	31.71 %	21.95 %	17.07 %	15.85 %
Falla o caídas del servicio	19.51 %	28.05 %	29.27 %	12.20 %	10.98 %

Fuente. Elaboración propia

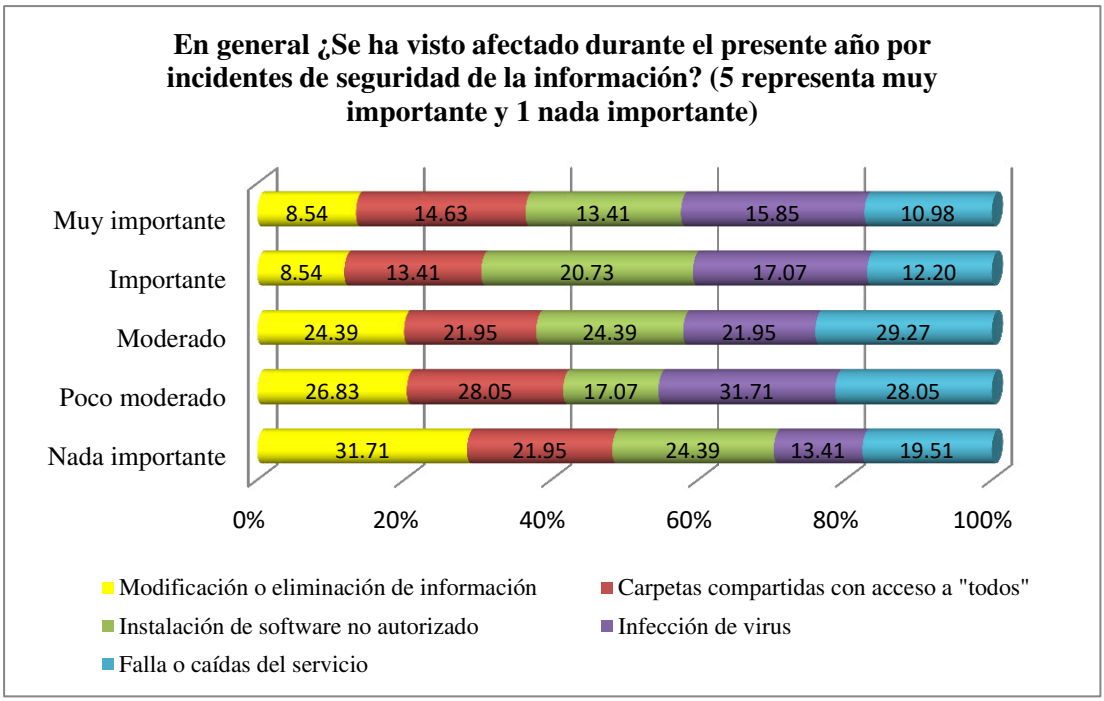


Figura 9: En general ¿Se ha visto afectado durante el presente año por incidentes de seguridad de la información?

Fuente. Elaboración propia

Cuadro 13 Estadísticas pregunta 6

–	Mínimo	Máximo	Mediana	Media	Desviación estándar
Modificación o eliminación de información	1,00	5,00	2,00	2,35	1,24
Carpetas compartidas con acceso a "todos"	1,00	5,00	2,00	2,68	1,32
Instalación de software no autorizado	1,00	5,00	3,00	2,79	1,37
Infección de virus	1,00	5,00	3,00	2,93	1,27
Falla o caídas del servicio	1,00	5,00	3,00	2,67	1,24

Fuente. Elaboración propia

Interpretación:

El principal incidente de seguridad de la información se encuentra las caídas o fallas del servicio seguido muy de cerca carpetas compartidas con acceso a

"todos", considerados dentro de los impactos como "moderado", es decir son las incidencias que suceden con mayor frecuencia.

7. **En general. Las consecuencias si se perdiera, comprometiera o no estuviese disponible información sensible de su empresa podría ocasionar. (Marque desde poco importante a muy importante).**

Cuadro 14 Encuesta pregunta 7

Opciones de Respuesta	Poco	Poco moderado	Moderado	Importante	Muy importante
Sanciones o multas legal o regulatorio	11.0	19.5	31.7	18.3	19.5
Pérdida de clientes	7.3	19.5	29.3	26.8	17.1
Daño a la reputación o imagen	8.5	14.6	32.9	18.3	25.6
Pérdida de ingresos	7.3	12.2	26.8	25.6	28.0
Daño en la relación con los empleados	20.7	23.2	23.2	22.0	11.0

Fuente. Elaboración propia

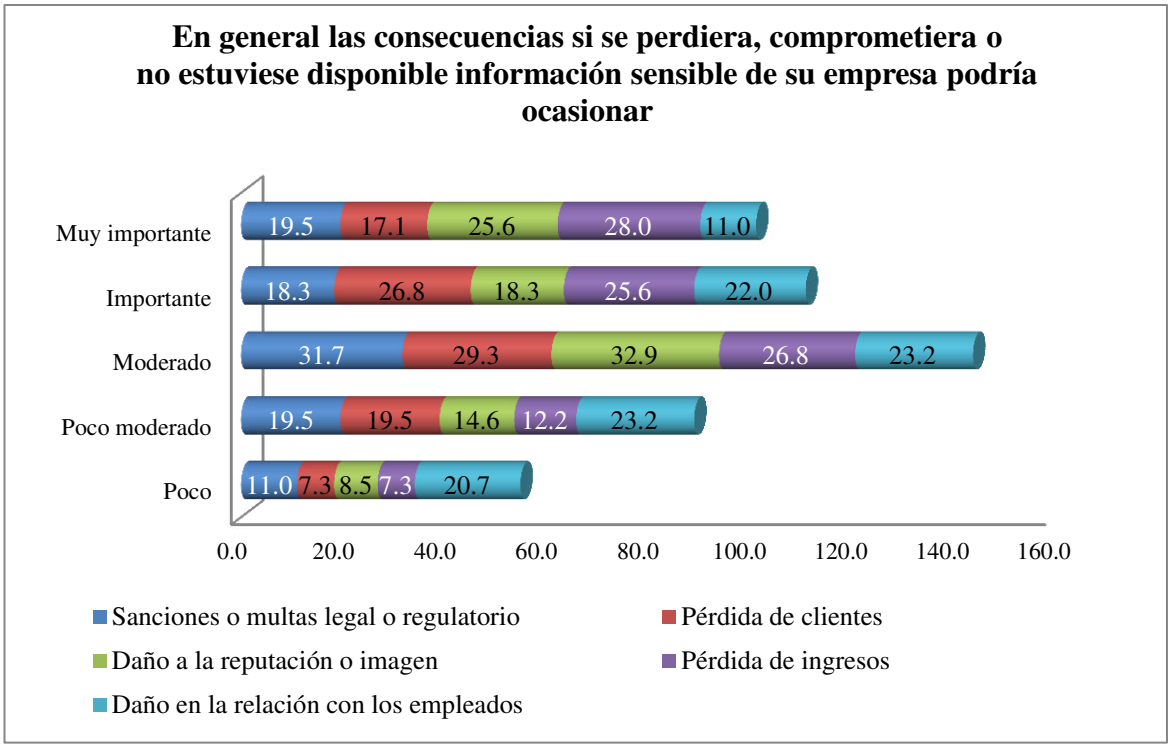


Figura 10: En general las consecuencias si se perdiera, comprometiera o no estuviese disponible información sensible de su empresa podría ocasionar

Fuente. Elaboración propia

Cuadro 15 Estadística pregunta 7

–	Mínimo	Máximo	Mediana	Media	Desviación estándar
Sanciones o multas legal o regulatorio	1,00	5,00	3,00	3,16	1,25
Pérdida de clientes	1,00	5,00	3,00	3,27	1,17
Daño a la reputación o imagen	1,00	5,00	3,00	3,38	1,25
Pérdida de ingresos	1,00	5,00	4,00	3,55	1,22
Daño en la relación con los empleados	1,00	5,00	3,00	2,79	1,29

Fuente. Elaboración propia

Interpretación:

Realizando un breve análisis con respecto a la disponibilidad de la información, es de mencionar de producirse algún evento adverso que afecta o pudiera afectar los activos de información, podría convertirse en una fuente de riesgo como se detalla a continuación:

- Sanciones o multas regulatorios o legales: El mayor índice es de impacto moderado.
- Pérdida de clientes: El mayor índice es de impacto moderado.
- Daño a la reputación o imagen: El mayor índice es de impacto moderado.
- Pérdida de ingresos: El mayor índice es de impacto muy importante.
- Daño a la relación con los empleados: Existe una igual entre moderado y poco moderado.

Por lo tanto el mayor riesgo por la falta de disponibilidad de la información es la pérdida de ingresos económicos.

8. ¿Cuál considera Ud. es el origen de los riesgos de seguridad de información reportado en su organización?

Cuadro 16 Encuesta pregunta 8

Opciones de Respuesta	Porcentaje de Respuesta	Conteo de Respuesta
Empleados	36.6%	30
Proveedores, consultores o contratas	15.9%	13
Hackers o atacantes	24.4%	20
Ex empleados	15.9%	13
Otros	7.3%	6

Fuente. Elaboración propia

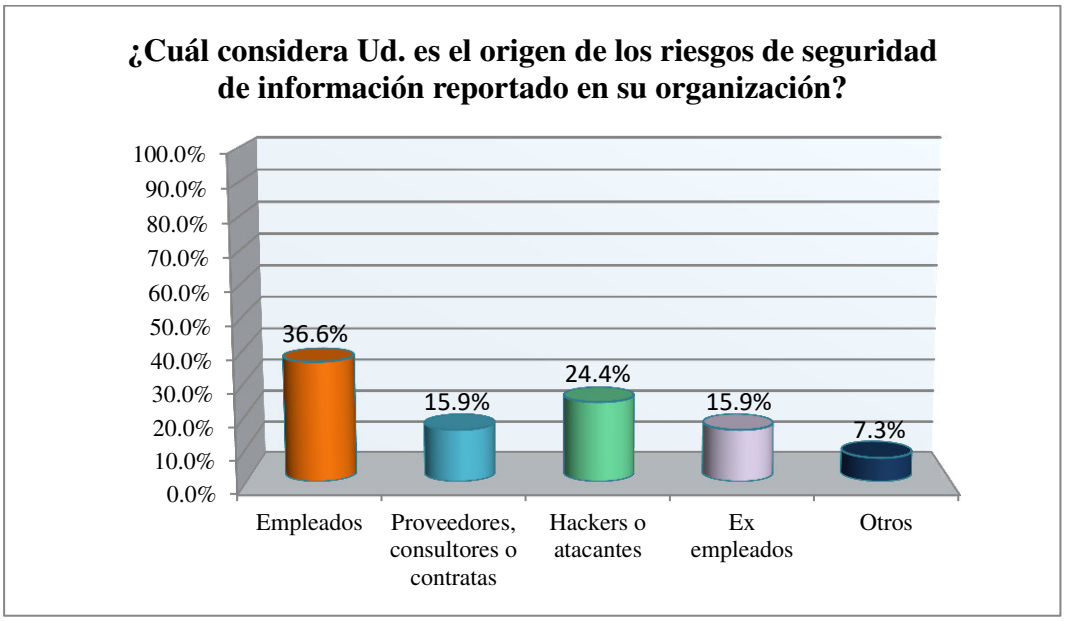


Figura 11: ¿Cuál considera Ud. es el origen de los riesgos de seguridad de información reportado en su organización?

Fuente. Elaboración propia

Interpretación:

Según la encuesta realizada en referencia al origen de los riesgos, el 36.6% considera que los empleados son los responsables de la explotación de los riesgos, debido a la falta de formación en seguridad de la información, falta de entrenamiento o talleres relacionado al tema, luego se encuentra los ataques externos con un 24.4%, debido a fallas técnicas (manipulación de sistemas de información, falta de monitoreo de los registros de las operaciones críticas, desconfiguración de dispositivos de seguridad, otros) y en menor medida personal cesado, personal externo y otros.

9. En general, ¿Cuántos riesgos han sido gestionados de forma anticipada y han evitado impactos, que generen pérdidas a la proyección estratégica de su empresa?

Cuadro 17 Encuesta pregunta 9

Opciones de Respuesta	Porcentaje de Respuesta	Conteo de Respuesta
Más de 5	28.0%	23
Menos de 5	17.1%	14
Ninguno	46.3%	38
Desconozco	8.5%	7

Fuente. Elaboración propia

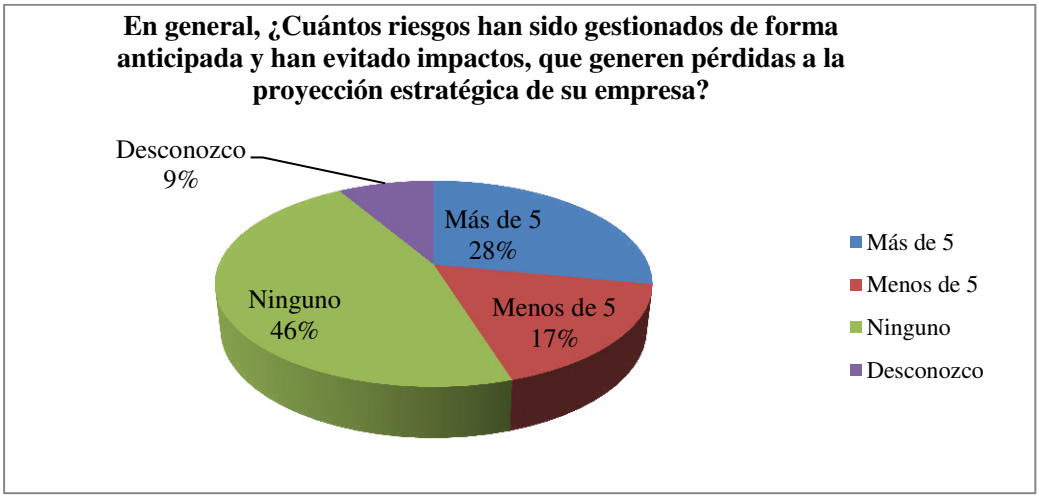


Figura 12: En general, ¿Cuántos riesgos han sido gestionados de forma anticipada y han evitado impactos, que generen pérdidas a la proyección estratégica de su empresa?

Fuente. Elaboración propia

Interpretación:

Del análisis realizado se valida, que el 46% afirma que no han tenido riesgos, esto podría significar que posiblemente los riesgos existen pero no han sido gestionados o también se podría interpretar que existe un desconocimiento sobre la existencia de riesgos y por lo tanto, no son considerados como temas relevantes en la planificación estratégica.

10. En su opinión ¿Hacia dónde considera usted que está orientada la inversión de gestión de riesgos en su empresa?

Cuadro 18 Encuesta pregunta 10

Opciones de Respuesta	Porcentaje de Respuesta	Conteo de Respuesta
Cumplimiento de políticas internas	29.3%	24
Capacitación y concientización de empleados	15.9%	13
Continuidad del negocio	25.6%	21
Consultoría	6.1%	5
Implementación de tecnología	17.1%	14
Otros	6.1%	5

Fuente. Elaboración propia

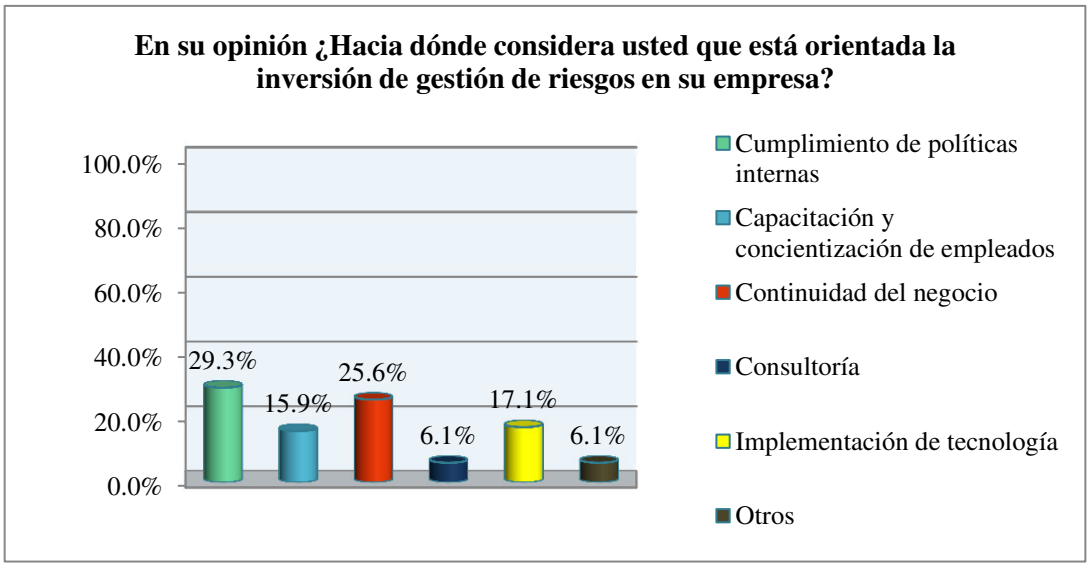


Figura 13: En su opinión ¿Hacia dónde considera usted que está orientada la inversión de gestión de riesgos en su empresa?

Fuente. Elaboración propia

Cuadro 19 Estadísticas básicas

Estadísticas básicas				
Mínimo	**Máximo**	**Mediana**	**Media**	**Desviación estándar**
1,00	6,00	3,00	2,84	1,61

Fuente. Elaboración propia

Interpretación:

Se muestra que el 29.3% considera que la inversión en la gestión de riesgos está orientada al cumplimiento de políticas internas, luego 25.6% considera que la Continuidad del Negocio es un factor importante en la inversión de los riesgos, luego la implementación de la tecnología y capacitación de colaboradores con 17.1% y 15.9% respectivamente y por último el 6.1% la inversión no se materializa en ninguno de los puntos expuestos.

4.2. Método de confiabilidad

El método de consistencia interna basado en el Alfa de Cronbach permite estimar la fiabilidad de un instrumento de medida a través de un conjunto de ítems que se espera que midan la misma dimensión teórica.

En una publicación los autores Oviedo & Campos (2005) coinciden "El valor mínimo aceptable para el coeficiente alfa de Cronbach es 0,70; por debajo de ese valor la consistencia interna de la escala utilizada es baja. Por su parte, el valor máximo esperado es 0,90; por encima de este valor se considera que hay redundancia o duplicación. Varios ítems están midiendo exactamente el mismo elemento de un constructo; por lo tanto, los ítems redundantes deben eliminarse. Usualmente, se prefieren valores de alfa entre 0,80 y 0,90 (…)". (Oviedo & Campos Arias, 2005, pág. 577)

4.3. Escala de Likert

Para la preguntas 6 y 7 de la encuesta se realizó bajo el escalamiento de Likert, según el autor Hernández Sampieri (2014) sostiene, "Consiste en un conjunto de ítems presentados en forma de afirmaciones o juicios, ante los cuales se pide la reacción de los participantes. Es decir, se presenta cada afirmación y se solicita al sujeto que externe su reacción eligiendo uno de los cinco puntos o categorías de la escala. A cada punto se le asigna un valor numérico. Así, el participante obtiene una puntuación respecto de la afirmación y al final su puntuación total, sumando las puntuaciones obtenidas en relación con todas las afirmaciones.". (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2014, pág. 238)

4.3.1. Resumen del procesamiento de los casos (a)

Este cuadro representa para 8 preguntas de la encuesta (se excluyen las preguntas 6 y 7 por ser realizadas bajo el escalamiento de Likert).

Cuadro 20 Resumen de procesamiento de casos (a)

Resumen de procesamiento de casos

		N	%
Casos	Válido	82	100,0
	Excluido[a]	0	,0
	Total	82	100,0

Fuente. Elaboración propia

Es de mencionar, que N hace referencia al total de encuestados (82) para realizar el procesamiento de datos.

Cuadro 21 Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,711	**8**

Fuente. Elaboración propia

Cabe mencionar, que el número de elementos N, hace referencia al total de preguntas consideradas en el procesamiento de datos. Por otro lado, los resultados obtenidos con el apoyo del software estadístico SPSS.

Cabe precisar, con los valores para los coeficientes de confiabilidad logrados, se puede afirmar que cumple con los estándares establecidos, con 0.711 de Alfa de Cronbach (cercanos al 1), orienta a garantizar el alto grado de fiabilidad de la escala.

4.3.2. Resumen del procesamiento de los casos (b)

Este cuadro representa las preguntas 6 y 7 (encuesta) por ser realizadas bajo el escalamiento de Likert.

Cuadro 22 Resumen de procesamiento de casos (a)

Resumen de procesamiento de casos

		N	%
Casos	Válido	80	97,6
	Excluido[a]	2	2,4
	Total	82	100,0

Fuente. Elaboración propia

Es de mencionar, que N hace referencia al total de encuestados (80) para realizar el procesamiento de datos, de los cuales dos (2) fueron excluidos.

Cuadro 23 Estadística de fiabilidad

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,797	**10**

Fuente. Elaboración propia

Cabe mencionar, que el número de elementos N, hace referencia al total de preguntas consideradas en el procesamiento de datos. Por otro lado, los resultados obtenidos con el apoyo del software estadístico SPSS.

Es de mencionar, que con los valores para los coeficientes de confiabilidad se puede afirmar que cumple con los estándares establecidos, con 0.797 de Alfa de Cronbach (cercanos al 1), lo que orienta a garantizar la fiabilidad de la escala.

4.4. Prueba de hipótesis

Luego de haber realizado la encuesta, es necesario comprobar la hipótesis planteada:

Hipótesis:

Una gestión de riesgos de seguridad de la información basada en un estándar internacional NTP ISO/IEC 31000 en las Empresas del sector Telecomunicaciones influye en el control de los riesgos de seguridad de la información.

4.4.1. Comprobación de Hipótesis General – Coeficiente de correlación de Pearson

El autor Hernández Sampieri (2014) hace referencia sobre el coeficiente de Pearson: "Es una prueba estadística para analizar la relación entre dos variables medidas en un nivel por intervalos o de razón. Se le conoce también como "coeficiente producto-momento"." (pág. 304)

Además, considera que se realiza el cálculo a través de la toma de una muestra de dos variables.

El autor añade, "Interpretación: el coeficiente r de Pearson puede variar de −1.00 a +1.00, donde: −1.00 = correlación negativa perfecta. ("A mayor X, menor Y", de manera proporcional. Es decir, cada vez que X aumenta una unidad, Y disminuye siempre una cantidad constante). Esto también se aplica "a menor X, mayor Y"." (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2014, pág. 305)

A continuación se muestran los resultados obtenidos, utilizando el software SPSS.

Cuadro 24 Correlación de Pearson

Correlaciones

		Seguridad de la Información	Gestión de Riesgos
Seguridad de la Información	Correlación de Pearson	1	,592**
	Sig. (bilateral)		,000
	N	82	82
Gestión de Riesgos	Correlación de Pearson	,592**	1
	Sig. (bilateral)	,000	
	N	82	82

**. La correlación es significativa al nivel 0,01 (bilateral).

Fuente. Elaboración propia

Interpretación:

Existe una correlación positiva media entre las variables gestión de riesgos y seguridad de la información (0.592) esto genera control de la información. Por lo tanto se puede afirmar que la hipótesis cumple la prueba.

Seguidamente, se toma las siguientes preguntas (extraídas de la encuesta) a fin de responder la hipótesis planteada, a través de la prueba de cola derecha, para

ver si la puntuación z está por debajo del punto de corte de nivel de significación. A continuación se muestra la figura 14.

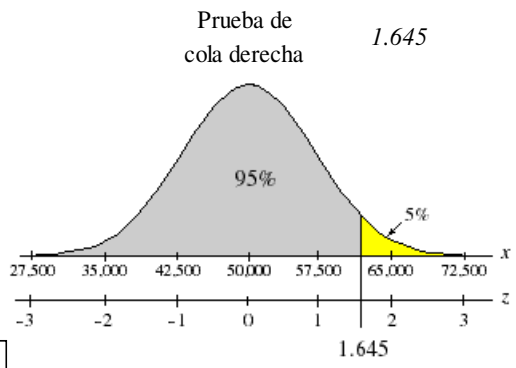
2. En general ¿Cuáles son los riesgos que se expone la organización en la inapropiada gestión de riesgos de seguridad de la información?

3. ¿Cuál de las siguientes tecnologías considera como la mayor preocupación de fuga de información?

H_1=	La inapropia gestión de accesos si conlleva a la fuga de información por el uso de herramientas tecnológicas
Ho=	La inapropia gestión de accesos no conlleva a la fuga de información por el uso de herramientas tecnológicas.
alfa α	0.05
confianza	95.00%

Datos

N1 = 82	N2= 82
$\overline{X}$= 2.05	$\overline{X}$= 1.80
S = 1.17	S = 1.01



$$Z = \chi 1 - X2 / \sqrt{\sigma^2 / n1 + \sigma^2 / n2}$$

Z: = 1.464666876

Regla de decisión: Rechazo Ho cuando Z es >1.65

Se acepta la hipótesis alternativa.

Figura 14: Comprobación de hipótesis

Fuente. Elaboración propia

Notas:

Ho: Hipótesis nula
H_1: Hipótesis alternativa
α: Nivel de significación
N1,N2: Población
$\overline{X}$: Media
S: Desviación estándar.

De lo anterior, se valida que la hipótesis alternativa describe que la ausencia de controles en la gestión de accesos, utilizando herramientas tecnológicas, podría conllevar a riesgos de seguridad de información. Es de mencionar, que las

preguntas formuladas corresponden como parte a los eventos identificados, señalados como de los problemas recurrentes en las empresas del sector Telecomunicaciones, objeto de la presente investigación. Por lo tanto, una gestión de riesgos de seguridad de la información basada en un estándar internacional NTP ISO/IEC 31000 en las Empresas del sector Telecomunicaciones influye en el control de los riesgos de seguridad de la información.

Capítulo 5 - IMPACTOS

5.1. Solución del problema: Gestión de riesgos para Telecomunicaciones.

El propósito de la Gestión de Riesgos de Seguridad de la Información es controlar los posibles riesgos que puede ser afectado una empresa. Transformar la incertidumbre de riesgos en seguridad mediante el desarrollo de la confianza utilizando métodos confiables generando un impacto significativo y positivo en sus operaciones internas, comerciales, legales o de reputación y evitar las multas o penalizaciones, pérdida de clientes, etc.

Resulta importante y fundamental la iniciativa y participación activa de la Alta Dirección en las diversas fases de la gestión de riesgos. Para ello, es necesario tener presente cuál es la estrategia de negocio de las empresas de este sector a fin de tener en claro cuáles son sus expectativas con relación a los riesgos.

Se toma en consideración, el análisis realizado es de orden cuantitativo, la identificación de los activos de información, amenazas y vulnerabilidades en la empresa se realizó de forma general; los controles y planes de acción fue definido sin considerar el impacto financiero, debido a la carencia de datos financieros, registros o documentos de sustento para realizar las estimaciones correspondientes; por lo tanto esta propuesta sirvió de guía para que la empresa y los responsables de los procesos y/o activos gestionen de manera apropiada los riesgos de seguridad de la información.

Se desea demostrar, que una gestión de riesgos de seguridad de la información basado en la NTP ISO/IEC 31000 permite controlar los riesgos en las empresas; y por lo tanto, aceptar la necesidad de implementar una gestión de riesgos de seguridad de la información en un entorno donde las amenazas y vulnerabilidades están cambiantes y su inadecuada gestión pueden ocasionar serios impactos en las empresas de este sector.

Este estudio se hace más interesante, debido a los grandes cambios que se han desarrollado en las últimas décadas, los riesgos existentes y nuevos en diferentes niveles como es la Seguridad de la Información, tecnología (Ciberseguridad), Seguridad Informática.

Es por ello, que una Gestión de Riesgos de Seguridad de la Información en empresas del sector Telecomunicaciones, con apoyo de estándares internacionales y su principal aporte a esta tesis es el cumplimiento con respecto al Secreto de las Telecomunicaciones, LPDP (Ley de Protección de Datos Personales) que toda empresa de este sector se encuentra obligada a cumplir para brindar servicios y operaciones en el país. Además, cubrir brechas relacionados a Ciberseguridad.

Adicional, se muestra la Figura 16 a fin de tener un panorama general del "Proceso de Gestión de Riesgos de Seguridad de la Información para empresas del sector Telecomunicaciones basado en la NTP ISO/IEC 31000".

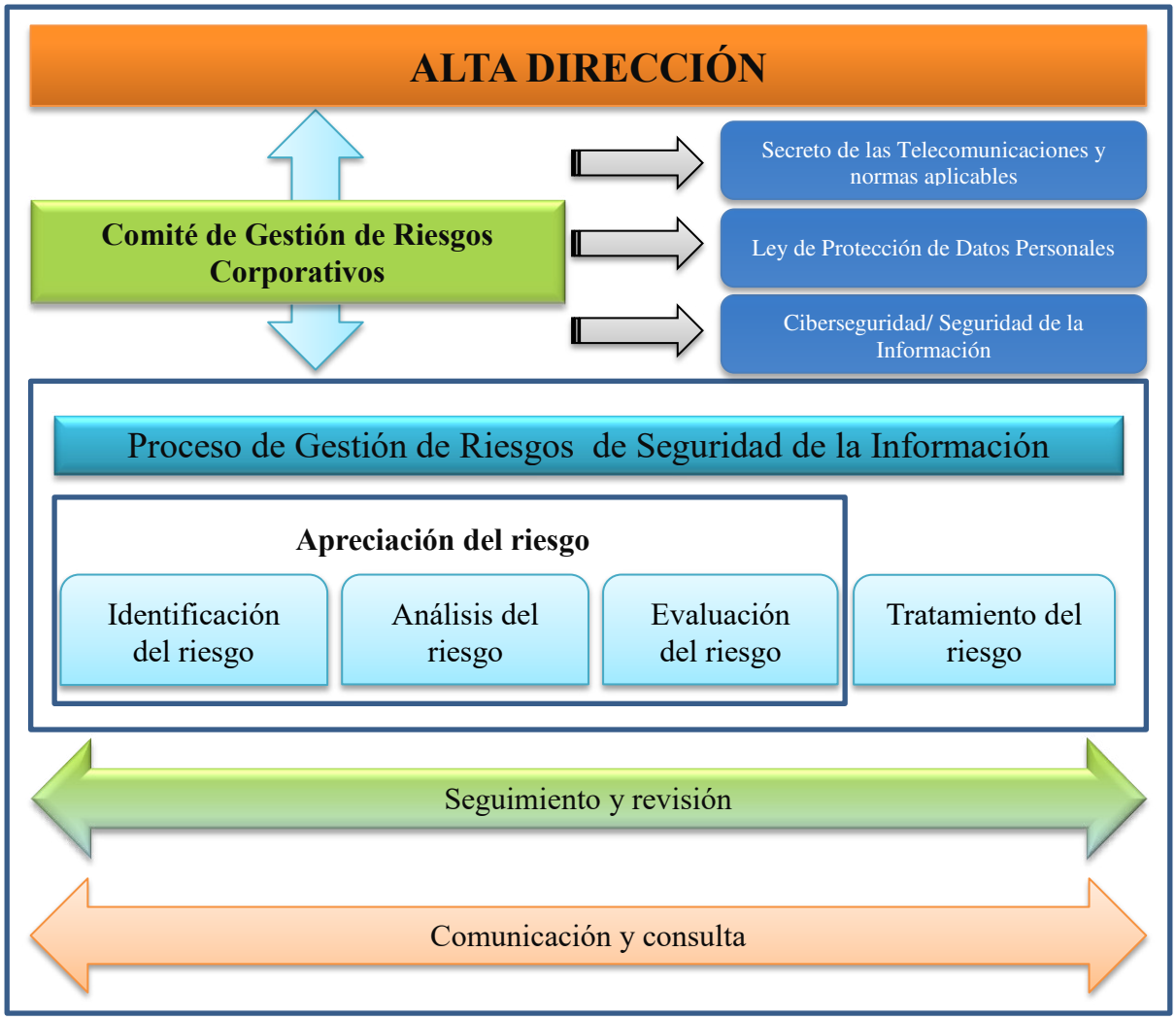


Figura 15: Proceso de Gestión de Riesgos de Seguridad de la Información para empresas del sector Telecomunicaciones basado en la NTP ISO/IEC 31000

Fuente. Elaboración propia

Para ejecutar, en referencia a la Figura 16 es importante describir los siguientes puntos referentes a un correcto proceso de gestión de riesgos, se indica a continuación:

A. Alta Dirección

Gestionar los riesgos en el sector de las Telecomunicaciones implica realizar ciertos cambios en la toma de decisiones, reingeniería, en todos sus niveles, desde la Alta Dirección pasando por todos los niveles de la empresa. Asimismo, es indispensable la participación activa e involucramiento de Gerentes, Directores que hacen parte de la Alta Dirección.

La Alta Dirección debe estar informada permanentemente de las actividades y gestiones realizadas por el Comité de Riesgos Corporativos para que sea posible la materialización de los proyectos e inversiones, oportunidades de mejora para que las empresas del sector Telecomunicaciones sigan brindando un servicio óptimo a los usuarios.

Adicional, tiene la decisión final de qué proceso, activo o área se realizará el proceso de gestión de riesgos.

La Alta Dirección es responsable de participar e impulsar a cada momento la administración del riesgo y ser un facilitador en la difusión de Políticas y Procedimientos internos a toda la empresa en todos sus niveles.

Además, tiene la decisión de establecer el contexto interno, externo, de los límites específicos de los riesgos de la empresa (aceptación del riesgo, tolerancia al riesgo) y en el caso de los riesgos identificados la decisión de su tratamiento.

B. Comité de Gestión de Riesgos Corporativos

Los miembros del Comité de Riesgos se recomienda que sean independientes de las funciones de la gestión de riesgos, con excepción de un líder que tenga los conocimientos necesarios en Seguridad, Riesgos, Incidentes, Continuidad de Negocio, entre otros (Jefe u Oficial de Seguridad de la Información).

En este Comité es necesario la participación de las principales áreas o gerencias de la empresa a fin que puedan tomar en consenso las acciones, actividades, inversiones, recursos para la Gestión de Riesgos de Seguridad de la Información.

Las leyes y/o regulaciones que son de cumplimiento obligatorio en el sector de Telecomunicaciones y son un factor importante para realizar cualquier tipo de actividad, a continuación, se detallan:

- Secreto de las Telecomunicaciones (leyes y/o regulaciones)
- Ley de Protección de Datos Personales.
- Ciberseguridad / Seguridad de la Información.

Como recomendación debería existir un Comité de Gestión de Riesgos, de no existir podría ser otro tipo de Comité (por ejemplo Comité de Riesgos Corporativos) que aborde estos temas, reporte directamente a la Alta Dirección e informe de las actividades derivadas del proceso de Gestión de Riesgos de Seguridad de la Información.

El Comité tiene la responsabilidad de delegar al área correspondiente de realizar el proceso de gestión de riesgos o en su defecto la contratación de un proveedor de servicios relacionados al tema.

El Comité debe proponer a la Alta Dirección los límites de aceptación al riesgo y apoyar y/o asesorar en el establecimiento del contexto.

Para complementar un proceso de riesgos, se puede delimitar el alcance a un proceso, activo o área y esta decisión es refrendada por la Alta Dirección.

C. Proceso de Gestión de Riesgos

Apreciación del Riesgo

Para comenzar, esta fase preliminar es donde se realiza las actividades operativas de gestión de riesgos que se enlistan:

- Entrevistas preliminares
- Relevamiento de información
- Comprensión del proceso
- Relevamiento de documentación existente (procedimientos, diagramas, registros).

a) Identificación de riesgos

Esta etapa corresponde a realizar las siguientes actividades:

- Entrevistas con los involucrados del proceso
- Conocimiento del proceso sin controles
- Proceso con controles
- Identificación de activos del proceso

- Inventario de activos y su clasificación
- Análisis y ponderación del nivel de criticidad de los activos
- Inventario de amenazas
- Inventario de vulnerabilidades
- Listado de riesgos
- Valoración del impacto y probabilidad de amenazas y vulnerabilidades

b) Análisis de riesgos

- Identificación de los riesgos asociados.
- Reuniones con la Alta Dirección
- Estrategia para abordar los riesgos

c) Evaluación de riesgos

- Reuniones con la Alta Dirección
- Priorización para tratamiento de los riesgos.

d) Tratamiento de riesgos

- Ejecución del Plan de Tratamiento de Riesgos (PTR). Acciones relacionados en la implementación de controles y seguimiento al mismo.

D. Seguimiento y revisión

Para las empresas del sector de Telecomunicaciones es importante acotar los requisitos indispensables para realizar de forma óptima el proceso de gestión de riesgos.

Es necesario precisar, en esta fase se realiza en todas las actividades de gestión de riesgos. Por ejemplo, se tiene que realizar un seguimiento de las actividades que están siendo ejecutadas, revisar si existe algún cambio en el contexto interno o externo de las empresas o se han presentado nuevos riesgos.

Cabe mencionar, en el siguiente cuadro sirve como medida de orientación a fin de tener un conocimiento general de todo el proceso de gestión de riesgos, es decir, desde la participación de la Alta Dirección hasta la etapa de seguimiento y revisión.

Los puntos o requisitos que pueden ser considerados como indispensables se detallan en el cuadro 25. Es preciso mencionar, que los requisitos pueden variar por diversas razones, por ejemplo, político, administrativo, legal u otro. Por lo tanto se debe tener identificado los requisitos para la gestión de riesgos en el ámbito de las telecomunicaciones.

Cuadro 25 Requisitos indispensables para la Gestión de Riesgos de Seguridad de la Información en empresas del sector Telecomunicaciones

Ítem	Actividad	¿Es necesario su		Observación
		Si	No	
A.	**Alta Dirección**	✓		En algunas empresas no lo definen como Alta Dirección, también podría ser considerado como Gerencia General, Gerente General, Directorio, Director u otro similar
B.	**Comité de Gestión de Riesgos**	✓		
	Secreto de Telecomunicaciones (Leyes y regulaciones)	✓		Requisito indispensable para las operaciones en el Perú
	Ley de Protección de Datos y su reglamento.	✓		Requisito indispensable que es de carácter mandatario para empresas privadas y públicas.
	Ciberseguridad		×	No es de carácter mandatario, pero debe ser considerado por el auge actual que está teniendo.
	Proceso de gestión de riesgos a abordar	✓		
	Proceso		×	El proceso de gestión de riesgos puede ser abordado a un proceso, activo o área
	Activo		×	El proceso de gestión de riesgos puede ser abordado a un proceso, activo o área
	Área		×	El proceso de gestión de riesgos puede ser abordado a un proceso, activo o área
C.	**Proceso de Gestión de Riesgos de Seguridad de la Información**	✓		
	Apreciación del Riesgos	✓		
	– Entrevistas preliminares	✓		
	– Relevamiento de información	✓		
	– Comprensión del proceso	✓		
	– Relevamiento de documentación existente (procedimientos, diagramas, registros).	✓		
	a) Identificación de riesgos	✓		
	b) Análisis de riesgos	✓		
	c) Evaluación de riesgos	✓		
D.	**Tratamiento de riegos**	✓		
E.	**Comunicación y consulta**	✓		
F.	**Seguimiento y revisión**	✓		

Fuente. Elaboración propia

E. Comunicación y consulta

Es necesario emitir e informar al Comité y a la Alta Dirección de todas las actividades importantes de la gestión de riesgos desde su inicio hasta su finalización.

Dependiendo de la cultura de la empresa estas comunicaciones podrían ser a través de reuniones semanales o mensuales según se defina, reportes o métricas de gestión o informes de periódicos del proceso de gestión de riesgos.

Por otro lado, en la figura 17, se muestra la metodología de gestión de riesgos genérica, tomando en referencia la NTP ISO/IEC 31000.

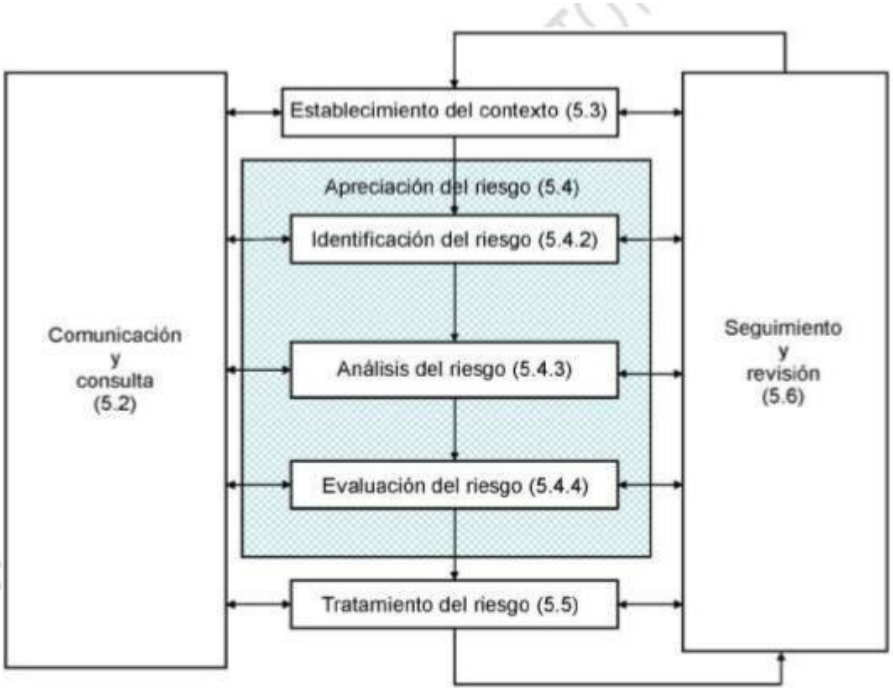


Figura 16: Proceso de gestión de riesgos basado en la ISO/IEC 31000

Fuente: (Norma Técnica Peruana NTP-ISO/IEC 31000:2011, 2011 Revisada 2016)

5.2. Implementación de Gestión de Riesgos de Seguridad de la Información para Telecomunicaciones

Cabe mencionar, para implementar la tesis "Gestión de Riesgos de Seguridad de la Información para empresas del sector Telecomunicaciones", se realizó la comprobación de la tesis en una empresa de Telecomunicaciones, por razones de confidencialidad no se brindará el nombre de la empresa, por lo tanto se tomará como supuesto el nombre de la empresa como "NETCOM".

5.3. Alta Dirección

En primer lugar, la Alta Dirección es el pilar y eje fundamental para implementar la gestión de riesgos en este sector, son los responsables de encaminar los proyectos, liderar, monitorear, impulsar, difundir, comunicar y definir el establecimiento del contexto con concordancia con el Comité de Riesgos.

Asimismo, su participación influye directamente en el cumplimiento de los objetivos trazados.

Establecimiento del contexto

En este punto es donde se articula los objetivos, se define el contexto interno y externo, alcance y los criterios de riesgo

Establecimiento del contexto interno

Son los requisitos internos que toda empresa debe tener identificado para el cumplimiento de sus objetivos. En el siguiente cuadro se brinda algunos puntos a tomar en consideración.

Cuadro 26 Contexto Interno

Contexto Interno	SI	No
Estructura interna (organigrama, estructura interna)	X	
Recursos humanos	X	
Políticas, misión, visión	X	
Filosofía, valores, objetivos y estrategias.	X	

Fuente. Elaboración propia

Establecimiento del contexto externo

Son los factores de índole externo que se deben considerar para lograr conseguir sus objetivos. A continuación se presenta algunos de los puntos a considerar:

Cuadro 27 Contexto Externo

Contexto Externo	SI	No
• Constitución Política • Artículos 161 y 162 del Código Penal • Ley de Telecomunicaciones • Reglamento General del Secreto de las Telecomunicaciones • Resolución Ministerial N° 111-2009-MTC/03 • Ley de Delitos Informáticos N° 30096 • Ley de Desarrollo de las Funciones y Facultades del OSIPTEL • Ley de Protección de Datos Personales N° 29733 y su Reglamento • Ley 27697 Ley que otorga facultad al Fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional	X	
Contratos con terceros	X	
Imagen Institucional	X	
Relaciones con el cliente	X	
Continuidad	X	

Fuente. Elaboración propia

5.4. Comité de riesgos

Para el desarrollo de la tesis no fue necesario la implementación de este Comité debido que la empresa NETCOM ya cuenta con un Comité de Riesgos Corporativos, los personas que conforman dicho Comité tienen el rango de Director o Gerente para ello se detalla:

- ✓ Gerente de Administración y Finanzas
- ✓ Gerente de Seguridad
- ✓ Gerente de Asesoría Legal
- ✓ Gerente de Auditoría Interna
- ✓ Gerente de Regulación
- ✓ Gerente de Tecnologías de Información
- ✓ Gerente de Recursos Humanos

5.4.1. Responsabilidades del Comité de Riesgos

Dentro de las siguientes actividades para iniciar una adecuada y correcta gestión de riesgos, se debe tomar en consideración los siguientes puntos:

- Enfrentar de manera efectiva la gestión de los riesgos, especialmente los de mayor impacto para la entidad, informando de ello a la Alta Dirección.
- Proponer a la Alta Dirección, tras su análisis y consideración, la gestión de riesgos, la cual identificará, al menos, los diversos niveles de riesgos; la fijación del nivel de riesgo aceptable; las medidas para mitigar el impacto de los riesgos identificados.
- Brindar soporte a los procesos críticos de la empresa.
- Adoptar el enfoque orientado a riesgos.

Asimismo, se estableció los criterios a tomar con relación al apetito y tolerancia de riesgo indicado en la Política de Gestión de Riesgos (documento interno de la empresa).

Por otro lado, es indispensable conocer de manera general la Matriz de Responsabilidades. Ver Anexo 9.7 (página 117).

5.4.2. Definición de los criterios de riesgo

Según la NTP ISO 31000 se debe "definir los criterios que se aplican para evaluar la importancia del riesgo. Los criterios deberían reflejar los valores, los objetivos y los recursos de la organización. Algunos criterios pueden estar impuestos o derivarse de requisitos legales o reglamentarios, o de otros requisitos suscritos por la organización. Los criterios de riesgo deberían ser coherentes con la política de gestión del riesgo de la organización". (Norma Técnica Peruana NTP-ISO/IEC 31000:2011, 2011 Revisada 2016, pág. 37).

Para ello ya se cuenta con la Política de Seguridad de la Seguridad, donde hace referencia sobre los criterios de riesgo, mostrados en los cuadros siguientes:

Cuadro 28 Categorías de Probabilidad

Categoría	Valor	Descripción
Casi seguro	5	Riesgo con probabilidad de ocurrencia es muy alto. (81% - 100%).
Muy probable	4	Riesgo con probabilidad de ocurrencia es alto. (51% - 80%)
Probable	3	Riesgo con probabilidad de ocurrencia media. (31% - 50%)
Poco probable	2	Riesgo con probabilidad de ocurrencia media. (11% - 30%)
Raro	1	Riesgo con probabilidad de ocurrencia muy baja. (0% - 10%)

Fuente. Elaboración propia

Cuadro 29 Categorías de Impacto

Categoría	Valor	Descripción
Mayor	5	Riesgo de materialización con altos impactos financieros, de reputación e imagen.
Importante	4	Riesgo de materialización con altos impactos financieros, de reputación e imagen.
Significativo	3	Riesgo de materialización con medianos impactos financieros, de reputación e imagen.
Regular	2	Riesgo de materialización con bajos impactos financieros, de reputación e imagen.
Menor	1	Riesgo de materialización con escasos impactos financieros, de reputación e imagen.

Fuente. Elaboración propia

Asimismo, el Comité estableció en consenso el proceso crítico al cual se realizará la gestión de riesgos.

También es necesario tomar en consideración los siguientes puntos:

a. Asignación recursos.

Se coordina con el área responsable de realizar la gestión de riesgos y Recursos Humanos a fin de evaluar personal temporal para apoyo de las actividades que demandará la gestión de riesgos.

b. Desembolso de presupuesto

La Alta Dirección destina el monto que será solicitado para la contratación de personal.

c. Inicio del proceso de riesgos

Inicio de las tareas a ejecutar.

d. Definición de los involucrados

Para el tema de la implementación la NETCOM ya cuenta con responsables de diferentes Direcciones de negocio que conforman la Alta Dirección entre ellos:

- ✓ Gerente General
- ✓ Director de Administración y Finanzas
- ✓ Director de Seguridad
- ✓ Director de Asesoría Legal
- ✓ Director de Auditoría Interna
- ✓ Director de Regulación
- ✓ Director de Sistemas de Información
- ✓ Director de Recursos Humanos

e. Responsabilidades principales de los involucrados

- Establecer los objetivos estratégicos.
- Aprobar las políticas que rigen a la empresa.
- Aprobar la creación de los Comités y Subcomités.
- Aprobar los presupuestos para la implementación de las mejoras de los procesos, controles necesario que deben implementarse en bien de la empresa.
- Monitorear el cumplimiento de los objetivos establecidos.
- Tomar las decisiones de cómo afrontar y priorizar los riesgos identificados.
- Asignar al personal idóneo.
- Realizar un monitoreo del proceso de riesgos.
- Evaluar los criterios riesgos en la empresa.
- Aprobar las posibles medidas para el tratamiento de los riesgos.

5.5. Apreciación del riesgo

Previo a la identificación de los riesgos, de realizó el relevamiento de información del proceso, fue necesario realizar una presentación (reunión) con el dueño del proceso a evaluar, se consideró los siguientes aspectos:

- ✓ Objetivo
- ✓ Alcance
- ✓ Metodología
- ✓ Actividades a realizar

Además, se realizó el conocimiento del proceso (entradas y salidas), a través de procedimientos establecidos o documentación que brindó el dueño del proceso (diagramas, flujos, procedimientos internos existentes, otros).

- Registros
- Muestras de información (documentos, procedimientos, formatos, otros).
- Otros.

Para efectos de la presente investigación se utilizó el enfoque bottom-up (de abajo - arriba), el cual permite un marco integral para ejecutar la gestión de riesgos.

En este punto fue necesaria la aplicación de las diversas técnicas de identificación de riesgos. En este caso fue necesario realizar diagramas de flujos, observación, entrevistas, aplicación de juicio de expertos.

5.5.1. Identificación del riesgo

En este punto se realiza la identificación de riesgos potenciales que podrían afectar a la empresa y por ende incumplir con sus objetivos, aquí se valida cuáles son los activos, áreas que requieren algún tipo de control.

Este punto del proceso de identificación de gestión de riesgos, es fundamental el compromiso de los dueños de los activos y/o procesos.

La NTP ISO/IEC 31000 estable “la identificación debería incluir los riesgos, tanto si su origen está o no bajo el control de la organización, incluso aunque el origen o la causa del riesgo no pueda ser evidente”. (Norma Técnica Peruana NTP-ISO/IEC 31000:2011, 2011 Revisada 2016, pág. 27)

Asimismo, los beneficios que genera esta actividad son:

- Identificación de activos que soporta el proceso
- Conocimiento actual de los procesos (con o sin controles).
- Análisis de posibles brechas en el proceso.
- Identificación de amenazas y vulnerabilidades.
- Oportunidades de mejora.

Además, es preciso realizar las siguientes actividades durante esta fase de la gestión:

A. Identificación de activos del proceso

Esta actividad se identificó los activos que hace parte del proceso crítico de la empresa, tomando en consideración los impactos con respecto a los pilares de la seguridad.

Cuadro 30 Inventario de activos del proceso

N°	ACTIVO
1	Solicitud de requerimientos
2	Reportes de base de datos
3	Actas de reuniones
4	Correo electrónico
5	Reportes
6	Contratos con Terceros
7	Matriz de actividades
8	Motor de Base de Datos
9	Sistema de Ventas
10	Datamart
11	Sistema de registro de pedidos
12	SAP
13	Oracle
14	Python
15	Sistema de Documentos
16	Visual Basic
17	SAS
18	Fox Pro
19	SPSS
20	Solar
21	FileZilla
22	Servidor SSH
23	Servidor FTP
24	Servidor SQL
25	File Server
26	Estaciones de trabajo
27	Dispositivo Móvil
28	Disco duro externo
29	Red de servicios
30	WI-FI
31	Proveedor de desarrollo
32	Proveedor de insumos
33	Personal
34	Oficinas
35	Imagen institucional
36	Cumplimiento

Fuente. Elaboración propia

B. Inventario de activos clasificados

En este punto se identificaron los activos que dan soporte a los procesos. Para ello se utilizó la clasificación propuesta por la ISO/IEC 27005. Se podrá clasificar los activos de TI, según sus características, se ha identificado los siguientes activos que dan soporte a NETCOM:

Cuadro 31 Inventario de los activos clasificados

N°	Tipo de Activo	ACTIVO
1	Información	Solicitud de requerimientos
2	Información	Reportes de base de datos
3	Información	Actas de reuniones
4	Información	Correo electrónico
5	Información	Reportes
6	Información	Contratos con Terceros
7	Información	Matriz de actividades
8	Software	Motor de Base de Datos
9	Software	Sistema de Ventas
10	Software	Datamart
11	Software	Sistema de registro de pedidos
12	Software	SAP
13	Software	Oracle
14	Software	Python
15	Software	Sistema de Documentos
16	Software	Visual Basic
17	Software	SAS
18	Software	Fox Pro
19	Software	SPSS
20	Software	Solar
21	Software	FileZilla
22	Hardware	Servidor SSH
23	Hardware	Servidor FTP
24	Hardware	Servidor SQL
25	Hardware	File Server
26	Hardware	Estaciones de trabajo
27	Hardware	Dispositivo Móvil
28	Hardware	Disco duro externo
29	Comunicaciones	Red de servicios
30	Comunicaciones	WI-FI
31	Servicios	Proveedor de desarrollo
32	Servicios	Proveedor de insumos
33	Recurso Humano	Personal
34	Infraestructura	Oficinas
35	Intangible	Imagen institucional
36	Intangible	Cumplimiento

Fuente. Elaboración propia

C. Definición de la criticidad de los activos

Asimismo, se realizó una definición de criticidad de cada activo en compañía del dueño del proceso en función a los 3 pilares de la seguridad.

Los valores asignados están relacionados con las definiciones y las decisiones que ha tomado la Alta Dirección.

Cuadro 32 Definición de la criticidad de los activos

N°	Tipo de Activo	ACTIVO	Criterios de seguridad		
			C	I	D
1	Información	Solicitud de requerimientos	4	3	3
2	Información	Reportes de base de datos	5	5	5
3	Información	Actas de reuniones	5	5	5
4	Información	Correo electrónico	5	4	4
5	Información	Reportes	5	5	5
6	Información	Contratos con Terceros	5	5	5
7	Información	Matriz de actividades	4	4	4
8	Software	Motor de Base de Datos	5	5	5
9	Software	Sistema de Ventas	5	5	5
10	Software	Datamart	5	5	5
11	Software	Sistema de registro de pedidos	4	4	4
12	Software	SAP	4	4	4
13	Software	Oracle	4	4	4
14	Software	Python	4	4	4
15	Software	Sistema de Documentos	5	5	5
16	Software	Visual Basic	5	5	5
17	Software	SAS	4	4	4
18	Software	Fox Pro	3	3	3
19	Software	SPSS	3	3	3
20	Software	Solar	3	2	2
21	Software	FileZilla	3	3	3
22	Hardware	Servidor SSH	5	5	5
23	Hardware	Servidor FTP	5	5	5
24	Hardware	Servidor SQL	5	5	5
25	Hardware	File Server	5	5	5
26	Hardware	Estaciones de trabajo	5	5	5
27	Hardware	Dispositivo Móvil	4	3	3
28	Hardware	Disco duro externo	5	5	5
29	Comunicaciones	Red de servicios	5	5	5
30	Comunicaciones	WI-FI	3	2	2
31	Servicios	Proveedor de desarrollo	5	5	5
32	Servicios	Proveedor de insumos	5	5	5
33	Recurso Humano	Personal	5	5	5
34	Infraestructura	Oficinas	3	3	3
35	Intangible	Imagen institucional	4	4	4
36	Intangible	Cumplimiento	4	4	4

Fuente. Elaboración propia

D. Inventario de amenazas.

Asimismo, se realizó un inventario de las posibles amenazas que podrían tener cada activo identificado.

En la publicación del Fondo de Tecnologías de Información y las Comunicaciones (2011), hace mención sobre las amenazas, “Una fuente de amenaza se define como cualquier circunstancia o evento con el potencial para causar daños a un sistema de TI. Las fuentes comunes de amenazas son las personas, la naturaleza y el ambiente”. (pág. 21)

(*) Se debe tomar en consideración que una amenaza puede afectar a uno o varios activos.

Ver el cuadro 33, donde se muestra el inventario de amenazas por activo detallado.

Cuadro 33 Inventario de amenazas por activo

N°	Activo	Amenazas
1	Solicitud de requerimientos	Fuga de información (divulgación, perdida o transferencia de información)
2	Reportes de base de datos	Fuga de información (divulgación, perdida o transferencia de información)
3	Actas de reuniones	Uso Inadecuado de activos
4	Correo electrónico	Degradación del equipo de comunicaciones o IT
5	Reportes	Fuga de información (divulgación, perdida o transferencia de información)
6	Contratos con Terceros	Fuga de información (divulgación, perdida o transferencia de información)
7	Matriz de actividades	Denegación de servicio
8	Motor de Base de Datos	Información sensible mal gestionada.
9	Sistema de Ventas	No disponibilidad/Falla en los datos de respaldos
10	Datamart	No disponibilidad/Falla en los datos de respaldos
11	Sistema de registro de pedidos	Denegación de servicio
12	SAP	Denegación de servicio
13	Oracle	Denegación de servicio
14	Python	Denegación de servicio
15	Sistema de Documentos	Denegación de servicio
16	Visual Basic	Denegación de servicio
17	SAS	Denegación de servicio
18	Fox Pro	Uso o conexión no autorizado / inapropiado de equipos y recursos informáticos / comunicaciones
19	SPSS	No disponibilidad/Falla en los datos de respaldos
20	Solar	Uso no autorizado de activos
21	FileZilla	No disponibilidad/Falla en los datos de respaldos
22	Servidor SSH	Uso Inadecuado de activos
23	Servidor FTP	Uso Inadecuado de activos
24	Servidor SQL	Exposición de información confidencial
25	File Server	Uso Inadecuado de activos
26	Estaciones de trabajo	Uso Inadecuado de activos
27	Dispositivo Móvil	Uso Inadecuado de activos
28	Disco duro externo	Código troyano, virus
29	Red de servicios	Fuga de información (divulgación, perdida o transferencia de información)
30	WI-FI	Uso o conexión no autorizado / inapropiado de equipos y recursos informáticos / comunicaciones
31	Proveedor de desarrollo	Incumplimiento de contrato
32	Proveedor de insumos	Incumplimiento de contrato
33	Personal	Robo de documentación/datos/extorsión
34	Oficinas	Terremoto/Inundación/Incendio/Terrorismo
35	Imagen institucional	Terremoto/Inundación/Incendio/Terrorismo
36	Cumplimiento	Sanciones

Fuente. Elaboración propia

E. Inventario de vulnerabilidades

Luego se realizó un inventario de las posibles vulnerabilidades que podrían afectar a cada activo.

En la publicación del Fondo de Tecnologías de Información y las Comunicaciones (2011), se toma en consideración su afirmación, “El análisis de las amenazas de un sistema de TI incluye el análisis de las vulnerabilidades asociadas al ambiente del sistema. La meta de este paso es desarrollar una lista de vulnerabilidades del sistema (defectos o debilidades) que podrían ser explotadas por fuentes de amenazas potenciales”. (pág. 23)

Cuadro 34 Inventario de vulnerabilidades por Activos y Amenazas

Activos	Amenazas	Vulnerabilidad
Solicitud de requerimientos	Fuga de información (divulgación, perdida o transferencia de información).	Falta de políticas, normas y procedimientos.
Reportes de base de datos	Fuga de información (divulgación, perdida o transferencia de información).	Uso no controlado de herramientas tecnológicas.
Actas de reuniones	Uso Inadecuado de activos.	Compartición de carpetas con acceso a "Todos" con información sensible.
Correo electrónico	Degradación del equipo de comunicaciones o IT.	No existencia de políticas de escritorio limpio.
Reportes	Fuga de información (divulgación, perdida o transferencia de información).	Compartición de carpetas con acceso a "Todos" con información sensible.
Contratos con Terceros	Fuga de información (divulgación, perdida o transferencia de información).	Brechas en las obligaciones definidas en los contratos.
Matriz de actividades	Denegación de servicio.	Brechas en las obligaciones definidas en los contratos.
Motor de Base de Datos	Información sensible mal gestionada.	Extracción de información confidencial o sensible por equipos y/o dispositivos no controlados o no inventariados.
Sistema de Ventas	No disponibilidad/Falla en los datos de respaldos.	Falta de registros de auditoría.
Datamart	No disponibilidad/Falla en los datos de respaldos.	Incumplimiento de los acuerdos de servicios.
Sistema de registro de pedidos	Denegación de servicio.	Compartición de carpetas con acceso a "Todos" con información sensible.
SAP	Denegación de servicio.	Falta/Desactualización de documentación de los procesos.
Oracle	Denegación de servicio.	Falta/Desactualización de documentación de los procesos.
Python	Denegación de servicio.	Falta/Desactualización de documentación de los procesos.

Activos	Amenazas	Vulnerabilidad
Sistema de Documentos	Denegación de servicio.	Control de acceso inadecuado.
Visual Basic	Denegación de servicio.	Control de acceso inadecuado.
SAS	Denegación de servicio.	Control de acceso inadecuado.
Fox Pro	Uso Inadecuado de activos.	Control de acceso inadecuado.
SPSS	No disponibilidad/Falla en los datos de respaldos.	Control de acceso inadecuado.
Solar	Exposición de los medios de almacenamiento.	Control de acceso inadecuado.
FileZilla	No disponibilidad/Falla en los datos de respaldos.	Falta de registros de auditoría.
Servidor SSH	Uso Inadecuado de activos.	Falta de registros de auditoría.
Servidor FTP	Uso Inadecuado de activos.	Incumplimiento de leyes o regulaciones.
Servidor SQL	Exposición de información confidencial.	Definición de roles inadecuadas.
File Server	Uso Inadecuado de activos.	Acceso no autorizado.
Estaciones de trabajo	Uso Inadecuado de activos.	Suplantación de identidad.
Dispositivo Móvil	Uso Inadecuado de activos.	Falta/Desactualización de documentación de los procesos.
Disco duro externo	Código troyano, virus.	Falta o incumplimiento de procedimientos para desecho/reutilización segura de equipos.
Red de servicios	Fuga de información (divulgación, perdida o transferencia de información).	Control de cambios inadecuado en la configuración.
WI-FI	Uso o conexión no autorizado / inapropiado de equipos y recursos informáticos / comunicaciones.	Falta de inventario de activos en forma periódica.
Proveedor de desarrollo	Incumplimiento de contrato.	Falta de auditoría en los procesos realizados en BI.
Proveedor de insumos	Incumplimiento de contrato.	Control de cambios inadecuado en la configuración.
Personal	Robo de documentación/datos.	Falta/falla/ robo o pérdida de control a los medios extraíbles.
Oficinas	Terremoto/Inundación/Incendio/Falla de suministro de respaldo (UPS)/Terrorismo.	Falta de mantenimiento/ Protección Física Inadecuada.
Imagen institucional	Terremoto/Inundación/Incendio/Falla de suministro de respaldo (UPS)/Terrorismo.	Desastre natural.
Cumplimiento	Sanciones.	Incumplimiento de leyes o regulaciones.

Fuente. Elaboración propia

F. Listado de riesgos

También, como para parte de las actividades se realizó un listado de riesgos que podrían afectar a los activos. A continuación se muestra el cuadro siguiente:

Cuadro 35 Listado de riesgos

Id	Listado de riesgos
1	Pérdida de oportunidades
2	Hacer peligrar la seguridad perimetral
3	Incumplimiento de restauración de información
4	Pérdida de la integridad de la información
5	Pérdida de la disponibilidad de la información
6	Costo interno adicional
7	Daños materiales
8	Falta de planes de continuidad
9	Perdida de la integridad de la información y/o información poco confiable
10	Transferencia de información por medios no seguros
11	Fuga de información - confidencialidad
12	Falta de trazabilidad
13	Extorsión o ataques a clientes
14	Procesos judiciales
15	Suplantación de identidad, préstamo de credenciales
16	Pérdida de la ventaja competitiva
17	Multas o penalidades
18	Incapacidad para prestar servicios.
19	Pérdida económica
20	Perdida de personal calificado o fuga de talentos
21	Perdida de la imagen, reputación y nombre de la empresa
22	Ausencia de segregación de funciones
23	Fraude
24	Falta de control de accesos (físicos y lógicos)
25	Crisis laboral, insatisfacción (huelga)

Fuente. Elaboración propia

G. Valoración del impacto y probabilidad de amenazas y vulnerabilidades

Es preciso señalar, en esta etapa se realiza un cálculo del impacto y la probabilidad de frecuencia con la finalidad de obtener la clasificación del riesgo a la que está expuesto el activo.

La valoración de riesgos permite:

1. Analizar el contexto orientado al negocio y su operación, y no en los componentes tecnológicos
2. Agrupar en dominios una lista de amenazas y vulnerabilidades y definir escenarios de posibles ataques
3. Seleccionar listas de controles para cada dominio que serán validadas a través de todo el sistema
4. Proveer y gestionar controles organizacionales y salvaguardas técnicas críticas y comunes.

Ver Anexo 9.8 (página 118).

5.5.2. Análisis del riesgo

La Norma Técnica Peruana NTP-ISO/IEC 31000:2011 (2011) señala: "El análisis del riesgo implica desarrollar una comprensión del riesgo. El análisis del riesgo proporciona elementos de entrada para la evaluación del riesgo y para tomar decisiones acerca de si es necesario tratar los riesgos, así como sobre las estrategias y los métodos de tratamiento del riesgo más apropiados (…)". (Norma Técnica Peruana NTP-ISO/IEC 31000:2011, 2011 Revisada 2016, pág. 39)

Para esta etapa del proceso de gestión de riesgos se realizó las siguientes actividades:

a. Identificación de los riesgos asociados.

Se detallan los riesgos que están afectados los activos de información de la empresa.

Ver Anexo 9.9 (página 121).

b. Estrategia para abordar los riesgos

En esta según NTP ISO/IEC 31000 "(…) El análisis del riesgo proporciona elementos de entrada para la evaluación del riesgo y para

tomar decisiones acerca de si es necesario tratar los riesgos, así como sobre las estrategias y los métodos de tratamiento del riesgo más apropiado". (Norma Técnica Peruana NTP-ISO/IEC 31000:2011, 2011 Revisada 2016)

La Alta Dirección selecciona las estrategias para abordar los riesgos: evitar, aceptar, reducir o compartir los riesgos, desarrollando una serie de medidas para adaptar los riesgos al perfil de riesgo de la entidad.

En esta etapa fue primordial la participación activa de la Alta Dirección, dado que ellos tomaron las estrategias para abordar los riesgos en conjunto con el consultor de riesgos a fin de brindar los detalles de los impactos que genera cada riesgo.

Ver Anexo 9.10 (página 126).

5.5.3. Evaluación del Riesgo

De la lista de los riesgos fue priorizar los riesgos de acuerdo con los criterios de evaluación del riesgo, se determinó los riesgos a tratar (decisión de la Alta Dirección) y la prioridad para implementar su tratamiento. Ver Anexo 9.11 (página 132).

Para la tesis de tomaron en consideración los riesgos clasificados como catastróficos, mayores y moderados.

Se revisa y analiza los riesgos a través de la matriz o mapa de calor (ver cuadro 36, cabe precisar que es solo referencial), y cuadro 37 sobre la prioridad de los riesgos.

Cuadro 36 Mapa de calor

Impacto	5. Catastrófico				12, 2	
	4. Mayor				11	
	3. Moderado			28, 5, 31, 32, 33, 6	24, 25, 3	
	2. Menor					
	1. Insignificante					
		0-10 %	11-30 %	31-50 %	51-80 %	81-100 %
		Raro	Improbable	Moderado	Probable	Casi cierto
		Probabilidad de ocurrencia				

Fuente. Elaboración propia

Cuadro 37 Prioridad de riesgos

Activos	Prioridad	Clasificación del Riesgo
SAP	79	Catastrófico
Sistema de registro de pedidos	51	Mayor
Servidor SQL	60	Moderado
File Server	58	Moderado
Disco duro externo	43	Moderado
Reportes de base de datos	52	Catastrófico
Actas de reuniones	51	Moderado
Reportes	49	Moderado
Proveedor de desarrollo	47	Moderado
Proveedor de insumos	47	Moderado
Personal	44	Moderado
Contratos con Terceros	42	Moderado

Fuente. Elaboración propia

Para priorizar los riesgos se tomaron en consideración los siguientes factores:

- Económico
- Continuidad
- Legal o regulatorio

- Imagen o reputación
- Contratos

5.6. Tratamiento de riesgos

Para la elaboración del Plan de Tratamiento de Riesgos (PTR) se tomaron en consideración los activos que representan un riesgo prioritario según se indica en el mapa de riegos.

La Norma Técnica Peruana NTP-ISO/IEC 31000:2011, señala "La selección de la opción más apropiada de tratamiento del riesgo implica obtener una compensación de los costes y los esfuerzos de implementación en función de las ventajas que se obtengan, teniendo en cuenta los requisitos legales, reglamentarios y de otro tipo (…)" (Norma Técnica Peruana NTP-ISO/IEC 31000:2011, 2011 Revisada 2016, pág. 39)

Para elaborar el Plan de Tratamiento de Riesgos (PTR), se tomó en consideración los controles de la ISO/IEC 27002 a fin de ejecutar el cumplimiento y gestionar de manera eficaz la gestión de riesgos (ver Anexo 9.12) página 134.

Luego de culminado las actividades de diseño de mitigación de riesgos corresponde a la Alta Dirección y los dueños de los procesos la implementación de los controles.

Para la presente tesis y por fines de tipo alcance, las actividades culminan en esta etapa. Logrando establecer un plan de trabajo coherente y efectivo que generará una nueva visión y rentabilidad en la empresa.

5.7. Seguimiento y revisión

Una vez evaluados los controles a implementar, de acuerdo al apetito de riesgo definido, sólo se evaluarán los niveles de riesgo que hayan obtenido valores de "Catastrófico", "Mayor" y "Moderado".

El monitoreo del riesgo a nivel de seguridad de la información, consiste en evaluar si el proceso es el apropiado y si existen nuevos riesgos o cambios en los existentes, que puedan ocasionar nuevas amenazas, vulnerabilidades o situaciones que se consideren inaceptables.

Esta gestión se realizó durante seis (06) meses, luego de definidos formalmente los controles y responsables.

5.8. Comunicación y consulta

Para esta fase se realizó planes de comunicación (reuniones semanales de los avances, verificación de cumplimiento de actividades, reuniones para definir los planes y tratamiento de riesgos), que cubrió desde el inicio hasta el cierre de la gestión de riesgos.

Es de mencionar, que las actividades comprendidas se ejecutaron de manera transversal, es decir, informar desde la Alta Dirección hasta los dueños de los activos y/o proceso.

5.9. Costos de implantación de la propuesta

Se presenta el cuadro siguiente, donde se muestra el costo referencial para implementación de la propuesta.

Cuadro 38 Costos de implantación de la propuesta

Recursos necesarios	**Costo S/.**
Personas (02)	48000
Otros gastos (materiales)	5000
Total	53000

Fuente. Elaboración propia

5.10. Beneficios que aporta la propuesta

Los beneficios que genera una Gestión de Riesgos de Seguridad de la Información en empresas del sector Telecomunicaciones son:

1. Realizando una oportuna gestión de riesgos, la NTP ISO/IEC 31000 por consiguiente, posibilita el cumplimiento de las exigencias legales, regulatorias y normas vigentes evitando penalidades por su incumplimiento (Secreto de las Telecomunicaciones, Protección de Datos Personales) e impactos en la imagen, reputación y mitigar posibles ataques relacionado a Ciberseguridad.
2. Es de mencionar, que la gestión de riesgos de seguridad de la información basada en la NTP ISO/IEC 31000 influye en el control de los riesgos en empresas del sector Telecomunicaciones.

3. Hay que mencionar, esta propuesta ayuda a concientizar sobre la necesidad de identificar, controlar y tratar los riesgos de seguridad de la información en todos los niveles de la empresa.
4. Mejora la toma de decisiones de la Alta Dirección a través de una gestión de riesgos de seguridad de la información
5. Mejora la identificación de oportunidades y amenazas.
6. Genera rentabilidad de las empresas a través de una gestión de riesgos de seguridad de la información.
7. Ayuda a reducir los posibles riesgos como: Impacto al Secreto de las Telecomunicaciones, incumplimiento de la Ley de Protección de Datos de Datos, fuga de información, pérdida de confidencialidad, ingeniería social, ataques de Ciberseguridad, entre otros.
8. A su vez, con el apoyo de la NTP ISO/IEC 31000 y la ISO/IEC 27005 es posible ser utilizada por cualquier organización de carácter público o privada para gestionar el riesgo de la seguridad de la información a nivel estratégico, proyectos, procesos, activos y servicios.
9. La gestión de riesgos de seguridad de la información, en definitiva apoya a incrementar la probabilidad de alcanzar los objetivos y generar rentabilidad y utilidad.
10. Apoya a la Alta Dirección a conseguir una solidez, en consecuencia podrá tomar decisiones oportunas.
11. Ayuda a mejorar o rediseñar los controles existentes, dimensionar los recursos oportunos para el tratamiento de riesgos.
12. Finalmente, permite ejercer un plan de acción oportuno ante los posibles incidentes de seguridad de la información y prevenir probables pérdidas económicas.

Capítulo 6 - CONCLUSIONES

Una Gestión de Riesgos de Seguridad de la Información en empresas del sector Telecomunicaciones, con apoyo de estándares internacionales como principal aporte a esta tesis es el cumplimiento con respecto a las principales Leyes que están sujetas y obligadas las empresas del sector Telecomunicaciones como es el Secreto de las Telecomunicaciones, la Ley de Protección de Datos Personales; a fin que puedan seguir operando y brindando servicios a personas naturales y jurídicas de todo el país. Además, permite el tratamiento oportuno de eventos relacionados a Ciberseguridad.

En la investigación realizada, se llegó como conclusión que una gestión de riesgos de Seguridad de la Información para Empresas del sector de Telecomunicaciones basada en un estándar internacional NTP ISO/IEC 31000 influye en el control de los riesgos en empresas del sector Telecomunicaciones. A su vez logra establecer normas para analizar de manera coherente los riesgos, facilitar indicadores y métricas de gestión que marquen el panorama actual de la empresa, y que sea un apoyo permanente a la Alta Dirección.

Con una correcta gestión de riesgos de Seguridad de la Información permite concluir el cumplimiento de los objetivos específicos; identificar los posibles riesgos de pérdida de información a través de una gestión de riesgos de seguridad de la información, mejorar la toma de decisiones de la Alta Dirección a través de una gestión de riesgos de seguridad de la información. Además, permite generar rentabilidad a través de una gestión de riesgos de seguridad de la información orientados a empresas del sector telecomunicaciones.

Asimismo, con la presente investigación se valida el cumplimiento de la hipótesis general planteada, asimismo de las hipótesis específicas.

Según la NTP ISO/IEC 31000 el éxito de la gestión del riesgo dependerá de la eficacia del marco de trabajo de gestión que proporcione las bases y las disposiciones que permitirán su integración a todos los niveles de la organización.

En la pregunta 3 de la encuesta realizada más de la mitad de los encuestados considera que la mayor preocupación en la fuga de información es el uso de medio de extraíbles con un 51.2%, en segundo lugar se muestra el uso de equipos móviles (26.8%) debido que estos aparatos cuentan con medio de grabación, fotografía y

almacenamiento de información, luego se aprecia el uso de los servicios en la nube (13.4%) que es una tecnología que está en crecimiento debido que no necesita medios físicos para almacenar o descargar información, luego se muestra el uso de software de control de escritorio (7.3%)permite acceder a otras estaciones de trabajo con la finalidad de extraer, eliminar o modificar información y por último el 1.2% considera que por otros medios se puede extraer información (uso de servidores de transferencia, correo electrónico, documentos impresos).

Adicional, en otras de las preguntas de la encuesta asociada a la Ley de Protección de Datos Personales en definitiva, preocupa que un poco más del 50% de los encuestados no tiene conocimiento sobre esta ley y sus implicancias en la salvaguarda de la información privada de los usuarios, el cual rige desde mayo del 2015, tanto la empresa privada o pública están obligadas su implementación.

La investigación tuvo una duración de seis (6) meses de ejecución el cual permite demostrar que utilizando la NTP ISO/IEC 31000 permite el incrementar el éxito de la gestión del riesgo e integración de todos los niveles de la empresa. Por ende permite fortalecer los controles existentes e implementar nuevos controles.

La adecuada Gestión de Riesgos de Seguridad de la Información genera retroalimentación, fortalecimiento y aprendizaje a toda la empresa y mejora la confianza de todos los involucrados (Comité, dueños de procesos y clientes).

Capítulo 7 - RECOMENDACIONES

1. Realizar una gestión de riesgos impulsado por la Alta Dirección y que las decisiones sean tomadas de manera metodológica con la finalidad que se cubran las brechas y cumplir con los objetivos plasmados.
2. Es importante que la Alta Dirección tenga identificado plenamente sus procesos, activos críticos a fin de lograr un entendimiento de las amenazas y vulnerabilidades de la empresa a fin de estar mejor preparada y prevenida para tomar decisiones en el momento oportuno. Se debe involucrar a los principales líderes de las áreas críticas, la participación activa de las áreas de Tecnologías de Información, Seguridad de la Información, Riesgos y Auditoría en los Comités, y en conjunto puedan tomar acción del adecuado plan para mitigar un riesgo.
3. Asimismo, realizar auditorías internas y externas con la finalidad de verificar el nivel de cumplimiento de las recomendaciones u observaciones identificadas. Esta actividad debe ser constante.
4. Realizar una "evaluación de madurez" permite a las empresas a identificar las amenazas que ponen en peligro la confidencialidad, integridad y disponibilidad de la información de la empresa en un momento dado y acompañado de la gestión de riesgos lograr oportunidades de mejoras, cierre de brechas el cual abarca no solo los aspectos tecnológicos sino que también incluye los procesos y las personas de las empresas. Tomar en consideración, evitar confundir el análisis de brechas con la gestión de riesgos ya que se trata de tareas que comparten el mismo objetivo de identificar las amenazas y deficiencias en la seguridad de la información en las empresas.

   El aporte de un análisis de brechas es tener el conocimiento de donde nos encontramos en este momento ante la implementación de la ISO/IEC 27001, sin embargo, si se desea conocer además cual es el esfuerzo necesario para ello se debe complementar este análisis con la gestión de riesgos para conocer el alcance real de la implementación de los controles.

5. Asimismo, tomar medidas de acción para el cumplimiento de las leyes y regulaciones que impactan directamente en las actividades de las empresas y

evitar que se vea afectada la imagen, reputación de las empresas del sector y por ende la confianza de clientes y proveedores.

6. Resulta crucial que las empresas inviertan en tecnología adecuada e implementen programas de cumplimiento basado en riesgos y desarrollen labores de capacitación a sus empleados para prevenir posibles ataques internos.
7. Es fundamental que las empresas de este sector mantengan un inventario de activos actualizado, verificado y validado por los dueños de los activos, con ello se podrá identificar de manera más clara y sencilla los posibles riesgos que puedan ser afectados.

Trabajos futuros

8. Un tema relevante que impacta o podría impactar a las empresas peruanas independientemente del sector o rubro de negocio a la que pertenecen es la Ciberseguridad dado sería un tema que podría ser abordado a mayor profundidad en futuras investigaciones.
9. La gestión de los riesgos es permanente y dinámica, se recomienda que las plantillas y formatos plasmados en la tesis sea implementada con una solución tecnológica (tomando en consideración la complejidad de la empresa) a fin de tener una visibilidad de las gestiones en tiempo real.

Capítulo 8 - REFERENCIAS BIBLIOGRÁFICAS

Aguilar, D. E. (2014). *Estudio para el Desarrollo de un Modelo de Gestión de Riesgos y Seguridad de la Información para Instituciones Militares.* Quito.

Arias Reyes, Y. L., Díaz Rodríguez, M. L., & Vargas Carvajal, J. A. Elaboración de una guía de Gestión de Riesgos basados en la Norma NTC-31000 para el proceso de Gestión de Incidentes y Peticiones del área de Mesa de Ayuda de Empresas de Servicio de Tecnología en Colombia. *Trabajo de Grado.* Universidad Católica de Colombia, Bogotá.

Arias Reyes, Y. L., Díaz Rodríguez, M. L., & Vargas Carvajal, J. A. (2014). *Elaboración de una guía de gestión de riesgos basados en la norma NTC-ISO 31000 para el proceso de gestión de incidentes y peticiones de servicio del área de mesa de ayuda de empresas de servicios de soporte de tecnología en Colombia.* Bogotá.

Bayona, A. R.-Z. (15 de Agosto de 2011). Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. *Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios.* Bogotá, Bogotá, Colombia.

Bayuk, J. (2018). El papel de la tecnología en la gestión del riesgo empresarial. *ISACA Journal*, 17.

Cano, J. (2014). La función de seguridad de la información. Presiones actuales y emergentes desde la inseguridad de la información. *ISACA Journal*, 1.

Casares San José - Martí, I. (2014). *Implementación de la Gestión Integral de Riesgos en el Sector Asegurador bajo la Norma ISO 31000.* Madrid: Molinuevo, Gráficos, S.L.

Casares San José Martí, I., & Lizarzaburu, B. E. (2016). *Introducción a la Gestión Integral de Riesgos Empresariales.* Lima: Platinum Editorial.

Casares San José Martí, I., & Lizarzaburu, B. E. (2016). *Introducción a la Gestión Integral de Riesgos Empresariales Enfoque: ISO 31000.* Lima: Platinum Editorial.

CIO Perú. (06 de 08 de 2018). *Ciberseguridad: ¿tendencia o necesidad?* Obtenido de CIO Perú: https://cioperu.pe/articulo/26340/ciberseguridad-tendencia-o-necesidad/

Congreso Constituyente Democrático. (1993). *Constitución Política del Perú.* Lima. Obtenido de Congreso: http://www4.congreso.gob.pe/ntley/Imagenes/Constitu/Cons1993.pdf

Congreso de la República. (17 de 07 de 2000). *https://www.osiptel.gob.pe/repositorioaps/data/1/1/1/par/ley27336-desarrollo-funciones-y-facultades-osiptel/Ley-27336-Ley-de-Desarrollo-de-Funciones-y-Facultades-del-OSIPTEL.PDF.* Obtenido de https://www.osiptel.gob.pe

Congreso de la República. (17 de 07 de 2000). *https://www.osiptel.gob.pe/repositorioaps/data/1/1/1/par/ley27336-desarrollo-funciones-y-facultades-osiptel/Ley-27336-Ley-de-Desarrollo-de-Funciones-y-Facultades-del-OSIPTEL.PDF.* Obtenido de https://www.osiptel.gob.pe/repositorioaps/data/1/1/1/par/ley27336-desarrollo-funciones-y-facultades-osiptel/Ley-27336-Ley-de-Desarrollo-de-Funciones-y-Facultades-del-OSIPTEL.PDF: https://www.osiptel.gob.pe/repositorioaps/data/1/1/1/par/ley27336-desarrollo-

funciones-y-facultades-osiptel/Ley-27336-Ley-de-Desarrollo-de-Funciones-y-Facultades-del-OSIPTEL.PDF

Congreso de la República. (2013). *Ley de Delitos Informáticos N° 30096.* Lima.

Congreso de la República del Perú. (1993). *http://www4.congreso.gob.pe/ntley/Imagenes/Constitu/Cons1993.pdf.* Obtenido de Congreso: http://www4.congreso.gob.pe/ntley/Imagenes/Constitu/Cons1993.pdf

Congreso de la República del Perú. (10 de Octubre de 2011). *https://www.minjus.gob.pe/wp-content/uploads/2013/04/LEY-29733.pdf.*

Congreso de la República del Perú. (2013). *Ley de Delitos Informáticos N° 30096.* Lima.

Congreso del Perú. (10 de 04 de 2002). *Ley que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional.* Lima. Obtenido de http://idehpucp.pucp.edu.pe/images/documentos/anticorrupcion/normativa/ley_facultades_fiscal.pdf

Congreso del Perú. (22 de 07 de 2007). *http://idehpucp.pucp.edu.pe/images/documentos/anticorrupcion/normativa/ley_facultades_fiscal.pdf.* Obtenido de http://idehpucp.pucp.edu.pe/images/documentos/anticorrupcion/normativa/ley_facultades_fiscal.pdf: http://idehpucp.pucp.edu.pe/images/documentos/anticorrupcion/normativa/ley_facultades_fiscal.pdf

Consejo de Auditoría Interna General de Gobierno. (2012). *Implantación, mantención y actualización del proceso de gestión de riesgos en el sector público.* Santiago.

COSO - Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise Risk Management Integrating with Strategy and Performance - Executive Summary.* USA.

COSO - Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise Risk Management Integrating with Strategy and Performance - Frequently Asked Questions.* USA.

COSO - Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Gestión del Riesgo Empresarial - Integrando Estrategia y Desempeño.* USA.

Devassy , J. T. (2016). Protegiendo la información— Estrategias prácticas para CIO y CISO. *ISACA Journal*, 34.

Devassy , J. T. (2016). Protegiendo la información— Estrategias prácticas para CIO y CISO. *ISACA Journal*, 34.

Di Lorio, A. H., Castellote, M. A., Constanzo, B., Curti, H., Waimann, J., Lamperti, S. B., . . . Nuñez, L. (2017). *El rastreo digital del delito - Aspectos técnicos, legales y estratégicos de la informática forense.* Mar del Plata: Universidad FASTA.

Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* España - Madrid: Ministerio de Hacienda y Administraciones Públicas.

Ernst & Young. (2018). En un mundo digital: ¿Sabe usted cuáles son los nuevos riesgos? *EY*, 92-93.

Ernst & Young. (2018). *En un mundo digital: ¿Sabe usted cuáles son los nuevos riesgos? Consideraciones clave para su plan de auditoría interna que*

ayudarán a la gerencia a dirigir en la era de la transformación. Lima: EYPerú Library.

Estévez Aguilar, D. P. Estudio para el desarrollo de un modelo de Gestión de Riesgos y Seguridad de la Información para Instituciones Militares. *Tesis de Maestría.* Escuela Politécnica Nacional, Quito.

Fondo de Tecnologías de Información y las Comunicaciones. (2011). *ANEXO 6: Metodología de Gestión del Riesgo - Modelo de Seguridad de la Información para la estrategia de Gobierno en linea 2.0.* Bogotá.

Freire Zapata, F. X. Implementación del Modelo de Gestión de la Seguridad de la Información aplicando ISO 27000 en la empresa Coka Tours, Ambato - Ecuador. *Trabajo de Maestría.* Universidad Central del Ecuador, Quito, Ecuador.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). *Metodología de la Investigación.* México: McGraw-Hill.

INCIBE - Instituto Nacioanl de Ciberseguridad. (2015). *Gestión de riesgos. Una guía de aproximación para el empresario.* España.

Instituto de Auditores Interno. (2017). *Marco Internacional para la Práctica Profesional de la Auditoría Interna.* Madrid: Instituto de Auditores Internos de España.

Instituto Nacional de Tecnologías de la Comunicación - Inteco. (2008). *Guía Avanzada de Gestión de Riesgos.*

ISACA. (2009). RISK IT - Marco de Riesgos de TI. En V. ISACA, *Marco de Riesgos de TI* (pág. 107). Chicago.

ISACA. (2012). *Cobit 5 Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa.* Chicago - Estados Unidos.

ISACA. (2013). *Transformando la Ciberseguridad* . Rolling Meadows, Illinois.

ISACA. (2017). *Cybersecurity Fundamentals Study Guide, 2nd Edition.* Rolling Meadows.

ISACA. (22 de 06 de 2018). *http://www.isaca.org*. Obtenido de http://www.isaca.org: http://www.isaca.org/spanish/Pages/default.aspx

ISO/IEC 27000:2018. (2018). *Tecnología de la información - Técnicas de seguridad - Sistemas de Gestión de la Seguridad de la Información - Generalidades y vocabulario.* Suiza, Suiza.

ISO/IEC 27001:2013. (2013). *La tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información.* Ginebra - Suiza.

ISO/IEC 27002:2013. (2013). *La tecnología de la información - Técnicas de seguridad - Código de práctica para los controles de seguridad de la información.* Ginebra - Suiza.

ISO/IEC 27005:2011. (2011). *Tecnología de la Información- Técnicas de Seguridad- La gestión de riesgos de seguridad de información.* Suiza.

ISO/IEC 27005:2018. (2018). *Tecnología de la Información- Técnicas de Seguridad- La gestión de riesgos de seguridad de información.* Suiza.

Martínez Rebollo, O. (2014). *Marco para el Gobierno de la Seguridad de la Información en servicios Cloud Computing.* Ciudad Real - España.

Megias Terol, J., Osuna García Malo de Molina, J., López Navarro, R., Cabañas Adame, A., Dahan García, N., Benito Gómez, M., & Simoni Granada, L. M. (2008). *Gestión estratégica de seguridad en la empresa.* Valencia: Filmac Centre S.L.

Merino Bada, C., & Cañizares Sales, R. (2011). *Implantación de un Sistema de Seguridad de la Información según ISO 27001.* España: Fundación Confemetal.

Ministerio de Justicia. (1993). *Texto Único Ordenado de la Ley de Telecomunicaciones* . Lima.

Ministerio de Justicia. (2007). *Decreto Supremo Nº 020-2007-MTC.* Lima.

Ministerio de Justicia y Derechos Humanos. (2013). *Directiva de Seguridad - Autoridad Nacional de Protección de Datos Personales APDP.* Lima: Editora Diskcopy S.A.C.

Ministerio de Justicia y Derechos Humanos. (2016). *Código Penal.* Lima: Biblioteca Nacional del Perú N° 2016-07121 .

Ministerio de Transportes y Comunicaciones. (2009). *Resolución Ministerial N° 11-2009-MTC/03.* Lima.

Norma Técnica Peruana NTP-ISO/IEC 31000:2011. (2011 Revisada 2016). *NTP ISO 31000:2016 Gestión del riesgo. Principios y directrices.* Lima.

Núñez Ponce, J. (11 de 03 de 2014). *Julio Nuñez Derecho Informático.* Obtenido de Julio Nuñez Derecho Informático: https://julionunezderechoinformatico.blogspot.com/search?q=30096

OCDE. (2018). *Política Regulatoria en el Perú: Uniendo el Marco para la Calidad Regulatoria, Revisiones de la.* París: Éditions OCDE.

Organismo Supervisor de Inversión Privada en Telecomunicaciones. (17 de 02 de 2016). *OSIPTEL.* Recuperado el 17 de Febrero de 2016, de https://www.osiptel.gob.pe

Organismo Supervisor de Inversión Privada en Telecomunicaciones. (9 de 10 de 2018). *OSIPTEL.* Recuperado el 17 de Febrero de 2016, de OSIPTEL: https://www.osiptel.gob.pe/categoria/enlaces-empresas-operadoras

Oviedo, H. C., & Campos Arias, A. (2005). *Metodología de investigación y lectura crítica de estudios - Aproximación al uso del coeficiente alfa de Cronbach.*

Oviedo, H. C., & Campos Arias, A. (2005). Metodología de investigación y lectura crítica de estudios - Aproximación al uso del coeficiente alfa de Cronbach. *Scielo*, 572-580.

Pallas Mega, G. Metodología de Implantación de un SGSI en un grupo empresarial jerárquico. *Tesis de Maestría.* Universidad de la República, Montevideo, Uruguay.

Pallas Mega, G. (2009). *Metodología de Implantación de un SGSI en un grupo empresarial jerárquico.* Montevideo - Uruguay.

Pastor Carrasco, C. (2010). *Impacto del riesgo en el Gobierno de Tecnologías de Información y Comunicación en la Gestión Empresarial industrial del siglo XXI.* Lima.

Pastor Carrasco, C. A. Impacto del riesgo en el Gobierno de Tecnologías de Información y Comunicación en la Gestión Empresarial industrial del siglo XXI. *Tesis de Maestría.* Universidad Nacional Mayor de San Marcos, Lima.

Piper, S. (2013). *Definitive Guide para la protección contra amenazas de próxima genereración.* Annapolis, Maryland: CyberEgde Group, LCC.

PricewaterhouseCoopers. (2018). Encuesta global sobre delitos económicos y fraude 2018. *PWC*, 2.

Rebollo Martínez, O. Marco para el Gobierno de la Seguridad de la Información en servicios Cloud Computing. *Tesis Doctoral.* Universidad de Castilla-La Mancha, Ciudad Real, España.

Sean, K. (2018). Construyendo puentes con el directorio - innovación en la gobernanza de la información. *ISACA Journal*, 35.

Seclen Arana, J. A. Factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001. *Tesis de Maestría.* Universidad Nacional Mayor de San Marcos, Lima.

Seclén Arana, J. A. (2016). *Factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001.* Lima – Perú.

Werneburg, M. (2017). Abordando riesgo compartido en las evaluaciones de vulnerabilidad de aplicaciones de productos. *ISACA Journal*, 43.

Wlosinski, L. G. (2017). Ingredientes clave para la planificación de la privacidad de la información. *ISACA Journal*, 39.

Zambrano Castillo, M., & Caro Perea, S. M. (2013). *Risk IT como complemento a la Gestión de Riesgos en Compañías de la Industria de Software.* Santiago de Cali.

Zámbrano Castillo, M., & Caro Perea, S. M. Risk IT como complemento a la Gestión de Riesgos en Compañías de la Industria de Software. *Maestría en Administración.* Universidad del Valle, Santiago de Cali.

Zapata, I. F. (2014). *Implementación del Modelo de Gestión de Seguridad de la Información aplicando ISO 27000 en la empresa Coka Tours, Ambato - Ecuador.* Quito - Ecuador.

Zárate Carlos, I. (2017). Comentarios a la Ley de Protección de Datos Personales (N° 29733). *Ingeniería Nacional - Revista Oficial del Colegio de Ingenieros del Perú*, 41-43.

Capítulo 9 - ANEXOS

9.1. Diagrama de Ishikawa

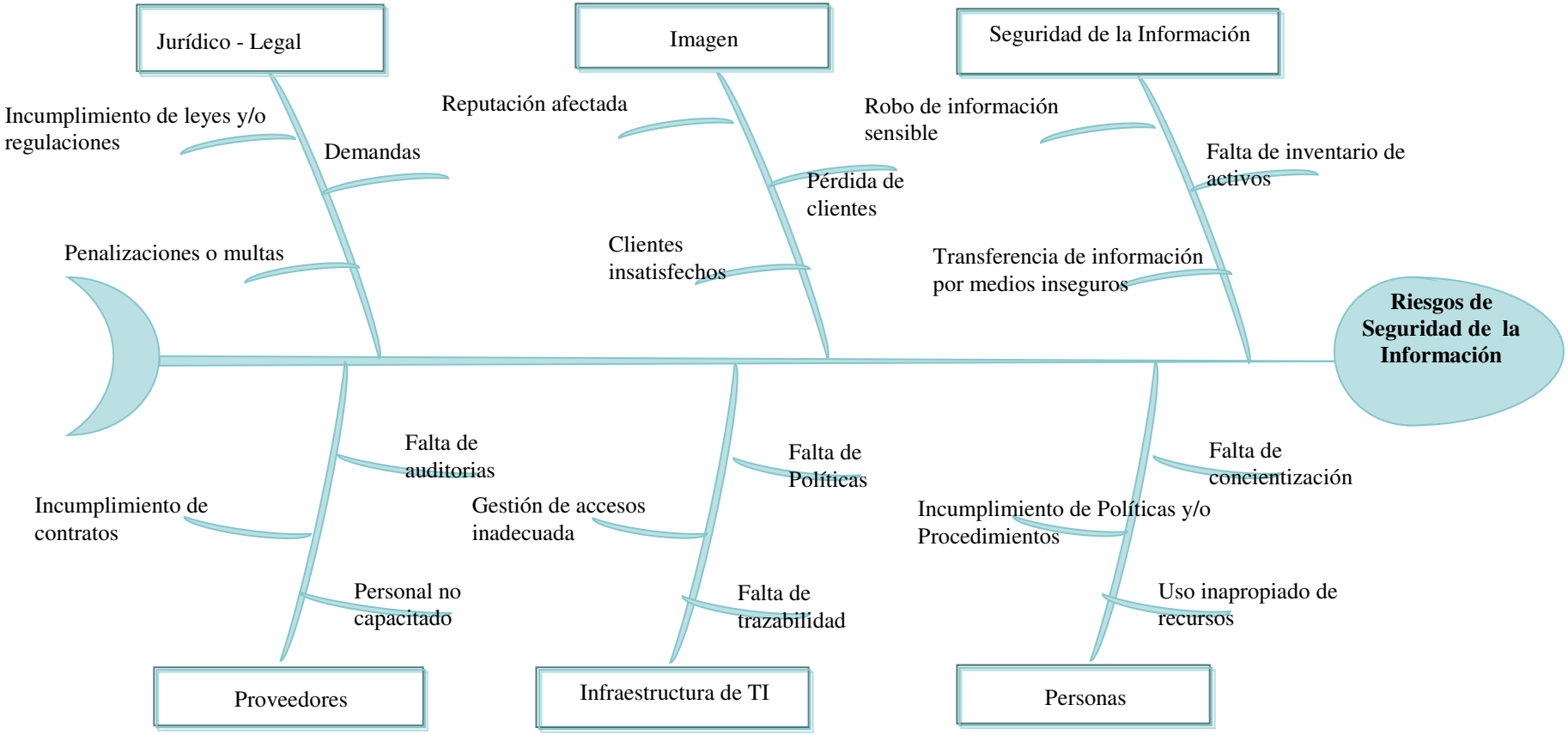


Figura 17 Diagrama de Ishikawa

Fuente. Elaboración propia

9.2. Matriz de consistencia

Cuadro 39 Matriz de Consistencia

GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN PARA EMPRESAS DEL SECTOR TELECOMUNICACIONES

Problema General	Objetivos	Hipótesis	Variables	Indicadores	Instrumentos de recopilación de información
¿De qué manera la gestión de riesgos de seguridad de la información basada en la NTP ISO/IEC 31000 influye en el control de los riesgos en empresas del sector Telecomunicaciones?	Determinar que la gestión de riesgos de seguridad de la información basada en la NTP ISO/IEC 31000 influye en el control de los riesgos en empresas del sector Telecomunicaciones.	Una gestión de riesgos de seguridad de la información basada en la NTP ISO/IEC 31000 en las empresas del sector Telecomunicaciones influye en el control de los riesgos de seguridad de la información.	**Variable X = Variable Independiente** Gestión de riesgos **Variable Y = Variable Dependiente**: Seguridad de la Información	Cantidad de riesgos identificados. % de riesgos mitigados.	Encuestas
Problemas Específicos	**Objetivos Específicos**	**Hipótesis específicas**	**Variables**	**Indicadores**	**Instrumentos de recopilación de información**
¿De qué manera la gestión de riesgos de seguridad de la información permite identificar los posibles riesgos de perdida de información?	Identificar los posibles riesgos de perdida de información a través de una gestión de riesgos de seguridad de la información.	Realizando una gestión de riesgos de seguridad de la información identifica los posibles riesgos de pérdida de información.	**Variable X = Variable Independiente** Gestión de riesgos **Variable Y = Variable Dependiente**: Pérdida de información.	Número de incidentes detectados de seguridad de la información. Número de amenazas identificadas. Número de vulnerabilidades.	Encuestas
¿De qué manera la gestión de riesgos de seguridad de la información mejora la toma decisiones de la Alta Dirección?	Obtener como mejora la toma de decisiones de la Alta Dirección a través de una gestión de riesgos de seguridad de la información.	Realizando una gestión de riesgos de seguridad de la información mejora la toma de decisiones de la Alta Dirección.	**Variable X = Variable Independiente** Gestión de riesgos **Variable Y = Variable Dependiente**: Toma de decisiones.	Cantidad de riesgos gestionados por la Alta Dirección.	Encuestas
¿De qué manera la gestión de riesgos de seguridad de la información permite generar rentabilidad a las empresas?	Generar rentabilidad de las empresas a través de una gestión de riesgos de seguridad de la información.	Realizando una gestión de riesgos de seguridad de la información genera rentabilidad en las empresas.	**Variable X = Variable Independiente** Gestión de riesgos **Variable Y = Variable Dependiente**: Rentabilidad de las empresas	% de inversión en planes de tratamiento de riesgos identificados.	Encuestas

Fuente. Elaboración Propia

9.3. Guía profesional general de los riesgos de TI

Sección	Subsección	Procesos de dominio del Marco de Referencia de Riesgos								
		RG1	RG2	RG3	RE1	RE2	RE3	RR	RR2	RR
1. Definición de un universo de riesgos y ámbito de gestión de riesgo.		RG1	RG2	RG3		RE2	RE3		RR2	
2. Apetito de riesgo y tolerancia al riesgo		RG1								
3.Conciencia del riesgo, Comunicación y presentación de informes	Conciencia del riesgo, Comunicación	RG1	RG2	RG3	RE1	RE2	RE3	RR1	RR2	RR3
	Principales indicadores del riesgo y presentación de informes						RE3	RR1	RR2	
	Perfil del riesgo						RE3			
	Agregación de riesgos	RG1	RG2	RG3				RR1		
	Cultura de riesgos	RG1	RG2							
4. Expresando y describiendo el riesgo	Introducción	RG1	RG2			RE2		RR1		
	Expresando su impacto en términos de negocios	RG1	RG2			RE2		RR1		
	Describiendo Riesgo-Expresando Frecuencia	RG1				RE2		RR1		
	Describiendo Riesgo-Expresando Impacto	RG1				RE2		RR1		
	Mapeando los objetivos de negocios de COBIT con otros criterios de impacto	RG1	RG2							
	Mapa de Riesgos	RG1					RE3	RR1		
	Registro de Riesgos						RE3			
5. Escenarios de riesgo	Explicación de los escenarios de riesgo	RG1				RE2	RE3			
	Ejemplo de escenarios de riesgo					RE2				
	Capacidad de Factores de Riesgo en el Proceso de Análisis de Riesgo	RG1			RE1	RE2	RE3			
	Factores de Riesgo Ambiental en el Proceso de Análisis de Riesgo	RG1			RE1	RE2				
Riesgo de respuesta y asignación de prioridades				RG3					RR2	RR3
7.Un flujo de trabajo de Análisis de Riesgo					RE1	RE2	RE3	RR1		
8. Mitigación de Riesgos de TI Uso de COBIT y VAL IT						RE2		RE1	RR2	RR3

Figura 18: Guía profesional general de los riesgos de TI

Fuente. (ISACA, 2009, pág. 36)

9.4. Modelo de encuesta

ENCUESTA

GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Nombres y Apellidos:_____
Cargo:_____
Empresa:_____

Por favor, dedique de 3 a 5 minutos a responder esta encuesta. Los resultados servirán para la investigación sobre gestión de riesgos de seguridad de la información.

Sus respuestas serán tratadas de forma CONFIDENCIAL Y ANÓNIMA. Es importante que responda con sinceridad.

Marque con una X la mejor alternativa. Por favor solo considere una alternativa.

1. **De manera general ¿Tiene conocimiento de la difusión y publicación de políticas o normativas de Seguridad de la Información/ Gestión de Riesgos?**
   1. Si
   2. No
   3. Desconozco
2. **En general ¿Cuáles son los riesgos que se expone de la organización en la inapropiada gestión de riesgos de seguridad de la información?**
   1. Fuga de información
   2. Acceso de personal no autorizado
   3. Fraudes
   4. Pérdida de la auditabilidad de la gestión
   5. Otros
3. **¿Cuál de las siguientes tecnologías considera como la mayor preocupación de fuga de información?**
   1. Medios extraíbles (USB, discos duros)
   2. Equipos móviles
   3. Servicios en la nube
   4. Software de control de escritorio
   5. Otros.
4. **En general ¿Tiene conocimiento de la Ley de Protección de Datos Personales Nº 29733?**
   1. Si
   2. No

3. Desconozco

5. ¿Se ha tenido en cuenta la seguridad de la información como criterio en las fases de desarrollo y puesta en producción de las aplicaciones usadas en los proyectos?

1. Si
2. No
3. A veces
4. Desconozco

6. En general ¿Se ha visto afectado durante el presente año por incidentes de seguridad de la información? (5 representa muy importante y 1 nada importante).

	Nada	Poco moderado	Moderado	Importante	Muy importante
Modificación o eliminación de información	○	○	○	○	○
Carpetas compartidas con acceso a "todos"	○	○	○	○	○
Instalación de software no autorizado	○	○	○	○	○
Infección de virus	○	○	○	○	○
Falla o caídas del servicio	○	○	○	○	○

7. En general. Las consecuencias si se perdiera, comprometiera o no estuviese disponible información sensible de su empresa podría ocasionar. (Marque desde poco importante a muy importante).

	Poco	Poco moderado	Moderado	Importante	Muy importante
Sanciones o multas legal o regulatorio	☐	☐	☐	☐	☐
Pérdida de clientes	☐	☐	☐	☐	☐
Daño a la reputación o imagen	☐	☐	☐	☐	☐
Pérdida de ingresos	☐	☐	☐	☐	☐
Daño en la relación con los empleados	☐	☐	☐	☐	☐

8. ¿Cuál considera Ud. es el origen de los riesgos de seguridad de información reportado en su organización?

1. Empleados
2. Proveedores, consultores o contratas
3. Hackers o atacantes
4. Ex empleados

5. Otros.

9. En general, ¿Cuántos riesgos han sido gestionados de forma anticipada y han evitado impactos, que generen pérdidas a la proyección estratégica de su empresa?

1. Más de 5
2. Menos de 5
3. Ninguno.
4. Desconozco.

10. En su opinión ¿Hacia dónde considera usted que está orientada la inversión de gestión de riesgos en su empresa?

1. Cumplimiento de políticas internas
2. Capacitación y concientización de empleados
3. Continuidad del negocio
4. Consultoría
5. Implementación de tecnología
6. Otros.

9.5. Ficha del informe de opinión de expertos

UNMSM- FCC
Investigación Aplicada II

Anexo: Ficha del Informe de opinión de expertos

I. DATOS GENERALES

1.1 Apellidos y Nombres del Informante : Darío Cóndor Callupe

1.2 Cargo e Institución donde labora : Coordinador de Seguridad de la Información - Telefónica Ingeniería de Seguridad S A

1.3 Título de la Investigación : Gestión de Riesgos de Seguridad de la Información para empresas del sector Telecomunicaciones

1.4 Nombre del instrumento : Encuesta

1.5 Autor del Instrumento : Miguel Humberto Huaura Mere

1.6 Maestría : Maestría Profesional en Gobierno de Tecnologías de Información

II. ASPECTOS DE VALIDACIÓN

INDICADORES	CRITERIOS	DEFICIENTE 00-20%	REGULAR 21-40%	BUENA 41-60%	MUY BUENA 61-80%	EXCELENTE 81-100%
1. CLARIDAD	Está formulado con lenguaje apropiado					X
2.OBJETIVIDAD	Está expresado en conductas observables				X	
3. ACTUALIDAD	Adecuado al avance de la ciencia y la tecnología				X	
4. ORGANIZACIÓN	Existe una organización lógica					X
5. SUFICIENCIA	Comprende los aspectos en cantidad y calidad				X	
6. INTENCIONALIDAD	Adecuado para valorar aspectos de la investigación					X
7. CONSISTENCIA	Basado en aspectos teórico-científicos de la investigación				X	
8. COHERENCIA	Entre los índices, indicadores y las dimensiones				X	
9. METODOLOGÍA	La estrategia responde al propósito del diagnóstico					X
10. PERTINENCIA	El instrumento es adecuado para el propósito de la investigación					X

III. OPINIÓN DE APLICABILIDAD

(.....) El Instrumento puede ser aplicado, tal como está elaborado
(.....) El Instrumento debe ser mejorado antes de ser aplicado, y nuevamente validado

IV. PROMEDIO DE VALORACIÓN: 88 %

Lugar y fecha: 04 de diciembre del 2015

Firma del experto informante
DNI N° 10122071 Telefono N° 690-1723

9.6. Modelo de instrumentación y matriz de operacionalización

Cuadro 40 Modelo de instrumentación y matriz de operacionalización

HIPÓTESIS GENERAL	VARIABLE		INDICADORES		ÍTEMS	ÍNDICES
Una gestión de riesgos de seguridad de la información basada en la NTP ISO/IEC 31000 en las empresas del sector Telecomunicaciones influye en el control de los riesgos de seguridad de la información.	X_0 Variable independientes	**GESTIÓN DE RIESGOS**	X_1	Número de riesgos identificados por su origen.	¿Cuál considera Ud. es el origen de los riesgos de seguridad de información reportado en su organización?	a) Empleados b) Proveedores o contratas c) Hackers o atacantes d) Ex empleados e) Otros.
			X_2	% riesgos por la inadecuada gestión de accesos.	En general ¿Cuáles son los riesgos que se expone de la organización por la inadecuada gestión de riesgos de seguridad de la información?	a) Fuga de información b) Acceso de personal no autorizado c) Fraudes d) Pérdida de la auditabilidad de la gestión e) Otros
			X_3	Número de riesgos gestionados	En general, ¿Cuántos riesgos han sido gestionados de forma anticipada y han evitado impactos, que generen pérdidas a la proyección estratégica de su empresa?	a) Más de 5 b) Menos de 5 c) Ninguno d) Desconozco
	Y_0 Variable dependiente	**SEGURIDAD DE LA INFORMACIÓN (control de riesgos)**	Y_1	% de proyectos que han considerado la seguridad de la información en sus desarrollos	¿Se ha tenido en cuenta la seguridad de la información como criterio en las fases de desarrollo y puesta en producción de las aplicaciones usadas en los proyectos?	a) Si b) No c) A veces d) Desconozco
			Y_2	% de riesgos críticos gestionados por la Alta Dirección.	¿Dónde se aborda la gestión de riesgos de seguridad de la información a nivel de Directorio?	a) Todo el Directorio b) Comité de Auditoría del Directorio c) Comité de Riesgos del Directorio d) No se aborda e) Otros
			Y_3	% de inversión en planes de tratamiento de riesgos.	En su opinión ¿Hacia dónde considera usted que está orientada la inversión para el tratamiento de riesgos en su empresa?	a) Cumplimiento de políticas internas b) Capacitación y concientización de empleados c) Continuidad del negocio d) Consultoría e) Implementación de tecnología f) Otros.

Fuente. Elaboración propia

9.7. Matriz de responsabilidades

Cuadro 41 Matriz de responsabilidades

Actividad		Roles			
ID	**Actividad**	**Alta Dirección**	**Comité**	**Dueños de procesos o activos**	**Gestor de riesgo**
1	**GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN**				
	Comunicación y consulta	I	I	I	R
	Establecimiento del contexto	R	R	R	R
	Apreciación del riesgo	A	A		R
	Identificación del riesgo	I	I	I	R
	Análisis de riesgos	A	C	I	R
	Valoración de riesgos	A	C		R
	Evaluación de Riesgos	A	I	I	R
	Tratamiento de riesgos	A	A		C
	Seguimiento y revisión	I	A		C

R: Responsable A: Aprobador C: Consultado I: Informado

Fuente: Elaboración propia

9.8. Valoración del impacto y probabilidad de amenazas y vulnerabilidades

Cuadro 42 Valoración del impacto y probabilidad de amenazas y vulnerabilidades

ID	Activos	Amenazas	Vulnerabilidad	Riesgo	Clasificación del Riesgo
1	Solicitud de requerimientos	Fuga de información (divulgación, perdida o transferencia de información)	Falta de políticas, normas y procedimientos	Perdida de la ventaja competitiva	Menor
2	Reportes de base de datos	Fuga de información (divulgación, perdida o transferencia de información)	Uso no controlado de información	Pérdida de oportunidades	Catastrófico
3	Actas de reuniones	Uso Inadecuado de activos	Compartición de carpetas con acceso a "Todos" con información sensible	Perdida de la disponibilidad de la información	Moderado
4	Correo electrónico	Degradación del equipo de comunicaciones o IT	No existencia de políticas de escritorio limpio	Fuga de información - confidencialidad	Menor
5	Reportes	Fuga de información (divulgación, perdida o transferencia de información)	Compartición de carpetas con acceso a "Todos" con información sensible	Perdida de la integridad de la información	Moderado
6	Contratos con Terceros	Fuga de información (divulgación, perdida o transferencia de información)	Brechas en las obligaciones definidas en los contratos	Pérdida económica	Moderado
7	Matriz de actividades	Información sensible mal gestionada.	Falta/Desactualización de documentación de los procesos.	Falta de trazabilidad/ Fuga de información	Insignificante
8	Motor de Base de Datos	Información sensible mal gestionada.	Extracción de información confidencial o sensible por equipos y/o dispositivos no controlados o no inventariados.	Costo interno adicional	Menor
9	Sistema de Ventas	No disponibilidad/Falla en los datos de respaldos	Registros de auditoría modificados.	Ausencia de trazabilidad. Fraudes. Transacciones indebidas.	Menor
10	Datamart	No disponibilidad/Falla en los datos de respaldos	Incumplimiento de los acuerdos de servicios	Falta de trazabilidad/ Fuga de información	Menor
11	Sistema de registro de pedidos	Denegación de servicio	Falta/Desactualización de documentación de los procesos.	Incumplimiento de procedimientos internos	Mayor
12	SAP	Denegación de servicio	Falta/Desactualización de documentación de los procesos.	Falta de trazabilidad/ Fuga de información	Catastrófico
13	Oracle	Denegación de servicio	Falta/Desactualización de documentación de los procesos.	Falta de trazabilidad	Menor

14	Python	Denegación de servicio	Falta/Desactualización de documentación de los procesos.	Falta de trazabilidad	Menor
15	Sistema de Documentos	Denegación de servicio	Control de acceso inadecuado	Suplantación de identidad, préstamo de credenciales	Menor
16	Visual Basic	Denegación de servicio	Control de acceso inadecuado	Suplantación de identidad, préstamo de credenciales	Menor
17	SAS	Denegación de servicio	Control de acceso inadecuado	Suplantación de identidad, préstamo de credenciales	Menor
18	Fox Pro	Uso Inadecuado de activos	Control de acceso inadecuado	Suplantación de identidad, préstamo de credenciales	Insignificante
19	SPSS	No disponibilidad/Falla en los datos de respaldos	Control de acceso inadecuado	Suplantación de identidad, préstamo de credenciales	Insignificante
20	Solar	Exposición de los medios de almacenamiento	Control de acceso inadecuado	Suplantación de identidad, préstamo de credenciales	Insignificante
21	FileZilla	No disponibilidad/Falla en los datos de respaldos	Falta de registros de auditoría	Multas o penalidades	Insignificante
22	Servidor SSH	Uso Inadecuado de activos	Falta de registros de auditoría	Falta de trazabilidad	Menor
23	Servidor FTP	Uso Inadecuado de activos	Incumplimiento de leyes o regulaciones	Pérdida económica Transferencia de información por medios no seguros.	Menor
24	Servidor SQL	Exposición de los medios de almacenamiento	Definiciones de roles inadecuadas	Falta de trazabilidad	Moderado
25	File Server	Uso Inadecuado de activos	Definiciones de roles inadecuadas	Falta de trazabilidad	Moderado
26	Estaciones de trabajo	Uso Inadecuado de activos	Definiciones de roles inadecuadas	Procesos judiciales	Menor
27	Dispositivo Móvil	Uso Inadecuado de activos	Falta/Desactualización de documentación de los procesos.	Transferencia de información por medios no seguros	Menor
28	Disco duro externo	Código troyano, virus	Falta o incumplimiento de procedimientos para desecho/reutilización segura de equipos	Multas o penalidades	Moderado
29	Red de servicios	Fuga de información (divulgación, perdida o transferencia de información)	Control de cambios inadecuado en la configuración	Incapacidad para prestar servicios.	Menor

30	WI-FI	Uso o conexión no autorizado / inapropiado de equipos y recursos informáticos / comunicaciones	Conexiones sin restricciones	Conexiones no autorizadas a la red	Insignificante
31	Proveedor de desarrollo	Incumplimiento de contrato	Falta de auditoría en los procesos realizados.	Incapacidad para prestar servicios.	Moderado
32	Proveedor de insumos	Incumplimiento de contrato	Control de cambios inadecuado en la configuración	Incapacidad para prestar servicios.	Moderado
33	Personal	Robo de documentación/datos	Falta/falla/ robo o pérdida de control a los medios extraíbles	Perdida de personal calificado o fuga de talentos. Falta de capacitación en seguridad de la información.	Moderado
34	Oficinas	Terremoto/Inundación/Incendio/Falla de suministro de respaldo (UPS)/Terrorismo	Falta de mantenimiento/ Protección Física Inadecuada	Falta de planes de continuidad	Menor
35	Imagen institucional	Terremoto/Inundación/Incendio/Falla de suministro de respaldo (UPS)/Terrorismo	Desastre natural	Daños materiales	Menor
36	Cumplimiento	Sanciones	Incumplimiento de leyes o regulaciones	Imagen alterada, reputación de la empresa. Pérdida de clientes. Multas o penalidades.	Menor

Fuente. Elaboración propia

9.9. Identificación de los riesgos asociados

Cuadro 43 Identificación de los riesgos asociados

ID	Activos	Tipo de Activo	Amenazas	Vulnerabilidad	Control Existente	Riesgo Asociado
A001	Solicitud de requerimientos	Información	Fuga de información (divulgación, perdida o transferencia de información)	Perdida de la ventaja competitiva	Se cuenta con un servidor de archivos, el cual es administrado por personal autorizado.	Perdida de la ventaja competitiva
A002	Reportes de base de datos	Información	Fuga de información (divulgación, perdida o transferencia de información)	Pérdida de oportunidades	No tiene controles.	Pérdida de oportunidades
A003	Actas de reuniones	Información	Uso Inadecuado de activos	Perdida de la disponibilidad de la información	Se tiene un repositorio de todas reuniones realizadas desde el 2014.	Perdida de la disponibilidad de la información
A004	Correo electrónico	Información	Degradación del equipo de comunicaciones o IT	Fuga de información - confidencialidad	Se mantiene un inventario de los respaldos generados, que son enviados periódicamente a un centro alterno según procedimientos internos.	Fuga de información - confidencialidad
A005	Reportes	Información	Fuga de información (divulgación, perdida o transferencia de información)	Perdida de la integridad de la información	No tiene controles.	Perdida de la integridad de la información
A006	Contratos con Terceros	Información	Fuga de información (divulgación, perdida o transferencia de información)	Pérdida económica	Se encuentra en revisión por área Legal.	Pérdida económica
A007	Matriz de actividades	Información	Información sensible mal gestionada.	Falta de trazabilidad/ Fuga de información	Se encuentra archivado en los discos locales.	Falta de trazabilidad/ Fuga de información

A008	Motor de Base de Datos	Software	Información sensible mal gestionada.	Costo interno adicional	Se cuenta con copias de seguridad de la Base de Datos. Monitoreo de los registros de auditoría. Control de accesos de usuarios.El acceso solo es con claves robustas.	Costo interno adicional
A009	Sistema de Ventas	Software	No disponibilidad/Falla en los datos de respaldos	Ausencia de trazabilidad.	Se cuenta con contratos de mantenimiento preventivo y correctivo con un proveedor. Se cuenta con copias de seguridad del sistema. Monitoreo de los registros de auditoría a nivel de usuarios y transacciones.	Ausencia de trazabilidad. Fraudes. Transacciones indebidas
A010	Datamart	Software	No disponibilidad/Falla en los datos de respaldos	Fraudes.	Se cuenta con copias de seguridad del sistema. Monitoreo de los registros de auditoría a nivel de usuarios y transacciones.	Falta de trazabilidad/ Fuga de información
A011	Sistema de registro de pedidos	Software	Denegación de servicio	Transacciones indebidas.	Se cuenta con copias de seguridad del sistema. Control de accesos de usuarios.	Incumplimiento de procedimientos internos
A012	SAP	Software	Denegación de servicio	Falta de trazabilidad/ Fuga de información	Se cuenta con copias de seguridad del sistema Control de accesos de usuarios.	Falta de trazabilidad/ Fuga de información
A013	Oracle	Software	Denegación de servicio	Incumplimiento de procedimientos internos	Se cuenta con contratos de mantenimiento preventivo y correctivo con un proveedor.	Falta de trazabilidad
A014	Python	Software	Denegación de servicio	Falta de trazabilidad/ Fuga de información	Se cuenta con copias de seguridad del sistema	Falta de trazabilidad
A015	Sistema de Documentos	Software	Denegación de servicio	Falta de trazabilidad	Se cuenta con copias de seguridad del sistema.	Suplantación de identidad, préstamo

					Control de accesos de usuarios.	de credenciales
A016	Visual Basic	Software	Denegación de servicio	Falta de trazabilidad	Se cuenta con copias de seguridad del sistema	Suplantación de identidad, préstamo de credenciales
A017	SAS	Software	Denegación de servicio	Suplantación de identidad, préstamo de credenciales	Se cuenta con copias de seguridad del sistema	Suplantación de identidad, préstamo de credenciales
A018	Fox Pro	Software	Uso Inadecuado de activos	Suplantación de identidad, préstamo de credenciales	Se cuenta con copias de seguridad del sistema	Suplantación de identidad, préstamo de credenciales
A019	SPSS	Software	No disponibilidad/Falla en los datos de respaldos	Suplantación de identidad, préstamo de credenciales	Se cuenta con copias de seguridad del sistema	Suplantación de identidad, préstamo de credenciales
A020	Solar	Software	Exposición de los medios de almacenamiento	Suplantación de identidad, préstamo de credenciales	Se cuenta con copias de seguridad del sistema. Monitoreo de los registros de auditoría.	Suplantación de identidad, préstamo de credenciales
A021	FileZilla	Software	No disponibilidad/Falla en los datos de respaldos	Suplantación de identidad, préstamo de credenciales	Se tiene un inventario de software autorizado.	Multas o penalidades
A022	Servidor SSH	Hardware	Uso Inadecuado de activos	Suplantación de identidad, préstamo de credenciales	Se tiene un plan de mantenimiento preventivo y correctivo. Se cuenta con control de accesos.	Falta de trazabilidad
A023	Servidor FTP	Hardware	Uso Inadecuado de activos	Multas o penalidades	Se tiene un plan de mantenimiento preventivo y correctivo. Se cuenta con control de accesos.	Pérdida económica. Transferencia de información por medios no seguros.
A024	Servidor SQL	Hardware	Exposición de los medios de	Falta de trazabilidad	Sala de servidores con controles	Falta de trazabilidad

			almacenamiento		ambientales	
A025	File Server	Hardware	Uso Inadecuado de activos	Pérdida económica	Se tiene control de carpetas compartidas de algunas áreas.	Falta de trazabilidad
A026	Estaciones de trabajo	Hardware	Uso Inadecuado de activos	Transferencia de información por medios no seguros.	Se cuenta con software antivirus instalado en toda la red. Las licencias se renuevan anualmente. Se realiza periódicamente depuración de carpetas compartidas y software no autorizado.	Procesos judiciales
A027	Dispositivo Móvil	Hardware	Uso Inadecuado de activos	Falta de trazabilidad	Se cuenta con la solución "Administración de Dispositivos Móviles".	Transferencia de información por medios no seguros
A028	Disco duro externo	Hardware	Código troyano, virus	Falta de trazabilidad	Se cuenta con la autorización del área de Seguridad de la Información.	Multas o penalidades
A029	Red de servicios	Comunicaciones	Fuga de información (divulgación, perdida o transferencia de información)	Procesos judiciales	Se tiene segmentado la red.	Incapacidad para prestar servicios.
A030	WI-FI	Comunicaciones	Uso o conexión no autorizado / inapropiado de equipos y recursos informáticos / comunicaciones	Transferencia de información por medios no seguros	Solo personal autorización tiene acceso al Wi-Fi.	Conexiones no autorizadas a la red
A031	Proveedor de desarrollo	Servicios	Incumplimiento de contrato	Multas o penalidades	Se cuenta con un contrato de servicios.	Incapacidad para prestar servicios.
A032	Proveedor de insumos	Servicios	Incumplimiento de contrato	Incapacidad para prestar servicios.	Se cuenta con un contrato de servicios.	Incapacidad para prestar servicios.

A033	Personal	Recurso Humano	Robo de documentación/datos	Conexiones no autorizadas a la red	Existe un plan de capacitación en seguridad de la información. Existen acuerdos de confidencialidad. Revisión anual de files del personal.	Perdida de personal calificado o fuga de talentos. Falta de capacitación en seguridad de la información.
A034	Oficinas	Infraestructura	Terremoto/Inundación/Incendio/Falla de suministro de respaldo (UPS)/Terrorismo	Incapacidad para prestar servicios.	Se cuenta con UPS. Se tiene un plan de continuidad ante incapacidad del servicio.	Deficiente planes de continuidad.
A035	Imagen institucional	Intangible	Terremoto/Inundación/Incendio/Falla de suministro de respaldo (UPS)/Terrorismo	Incapacidad para prestar servicios.	Se realizan pruebas de continuidad una vez al año.	Daños materiales.
A036	Cumplimiento	Intangible	Sanciones	Incumplimiento de leyes o regulaciones	Se tiene proveedor de servicios de vigilancia, quienes validan y registran las entradas y salidas a las zonas restringidas.	Perdida de la imagen, reputación y nombre de la empresa. Multas o penalidades.

Fuente. Elaboración propia

9.10. Estrategia para abordar los riesgos

Cuadro 44 Estrategia para abordar los riesgos

ID	Activos	Tipo de Activo	Amenazas	Vulnerabilidad	Control Existente	Riesgo Asociado	Clasificación del Riesgo	Estrategia
1	Solicitud de requerimientos	Información	Fuga de información (divulgación, perdida o transferencia de información)	Perdida de la ventaja competitiva	Se cuenta con un servidor de archivos, el cual es administrado por personal autorizado.	Perdida de la ventaja competitiva	Menor	Aceptar
2	Reportes de base de datos	Información	Fuga de información (divulgación, perdida o transferencia de información)	Pérdida de oportunidades	No tiene controles.	Pérdida de oportunidades Incumplimiento de leyes y regulaciones.	Catastrófico	Mitigar
3	Actas de reuniones	Información	Uso Inadecuado de activos	Perdida de la disponibilidad de la información	Se tiene un repositorio de todas reuniones realizadas desde el 2014.	Perdida de la disponibilidad de la información	Moderado	Mitigar
4	Correo electrónico	Información	Degradación del equipo de comunicaciones o IT	Fuga de información - confidencialidad	Se mantiene un inventario de los respaldos generados, que son enviados periódicamente a un centro alterno según procedimientos	Fuga de información - confidencialidad	Menor	Aceptar

					internos.			
5	Reportes	Información	Fuga de información (divulgación, perdida o transferencia de información)	Perdida de la integridad de la información	No tiene controles.	Perdida de la integridad de la información	Moderado	Mitigar
6	Contratos con Terceros	Información	Fuga de información (divulgación, perdida o transferencia de información)	Pérdida económica	Se encuentra en revisión por área Legal.	Pérdida económica	Moderado	Mitigar
7	Matriz de actividades	Información	Información sensible mal gestionada.	Falta de trazabilidad/ Fuga de información	Se encuentra archivado en los discos locales.	Falta de trazabilidad/ Fuga de información	Insignificante	Aceptar
8	Motor de Base de Datos	Software	Información sensible mal gestionada.	Costo interno adicional	Se cuenta con copias de seguridad de la Base de Datos.	Costo interno adicional Incumplimiento de leyes y regulaciones.	Menor	Aceptar
9	Sistema de Ventas	Software	No disponibilidad/Falla en los datos de respaldos	Ausencia de trazabilidad.	Monitoreo de los registros de auditoría.	Ausencia de trazabilidad. Fraudes. Transacciones indebidas	Menor	Aceptar
10	Datamart	Software	No disponibilidad/Falla en los datos de respaldos	Fraudes.	Control de accesos de usuarios. El acceso solo es con claves robustas.	Falta de trazabilidad/ Fuga de información	Menor	Aceptar
11	Sistema de registro de pedidos	Software	Denegación de servicio	Transacciones indebidas.	Se cuenta con contratos de mantenimiento preventivo y correctivo	Incumplimiento de procedimientos internos	Mayor	Mitigar

					con un proveedor.			
12	SAP	Software	Denegación de servicio	Falta de trazabilidad/ Fuga de información	Se cuenta con copias de seguridad del sistema.	Falta de trazabilidad/ Fuga de información Incumplimiento del Secreto de las Telecomunicaciones. Incumplimiento de la Ley de Protección de Datos Personales.	Catastrófico	Mitigar
13	Oracle	Software	Denegación de servicio	Incumplimiento de procedimientos internos	Monitoreo de los registros de auditoría a nivel de usuarios y transacciones.	Falta de trazabilidad	Menor	Aceptar
14	Python	Software	Denegación de servicio	Falta de trazabilidad/ Fuga de información	Se cuenta con copias de seguridad del sistema.	Falta de trazabilidad	Menor	Aceptar
15	Sistema de Documentos	Software	Denegación de servicio	Falta de trazabilidad	Monitoreo de los registros de auditoría a nivel de usuarios y transacciones.	Suplantación de identidad, préstamo de credenciales	Menor	Aceptar
16	Visual Basic	Software	Denegación de servicio	Falta de trazabilidad	Se cuenta con copias de seguridad del sistema.	Suplantación de identidad, préstamo de credenciales	Menor	Aceptar
17	SAS	Software	Denegación de servicio	Suplantación de identidad, préstamo de credenciales	Control de accesos de usuarios.	Suplantación de identidad, préstamo de credenciales	Menor	Aceptar

18	Fox Pro	Software	Uso Inadecuado de activos	Suplantación de identidad, préstamo de credenciales	Se cuenta con copias de seguridad del sistema	Suplantación de identidad, préstamo de credenciales	Insignificante	Aceptar
19	SPSS	Software	No disponibilidad/Falla en los datos de respaldos	Suplantación de identidad, préstamo de credenciales	Control de accesos de usuarios.	Suplantación de identidad, préstamo de credenciales	Insignificante	Aceptar
20	Solar	Software	Exposición de los medios de almacenamiento	Suplantación de identidad, préstamo de credenciales	Se cuenta con contratos de mantenimiento preventivo y correctivo con un proveedor.	Suplantación de identidad, préstamo de credenciales	Insignificante	Aceptar
21	FileZilla	Software	No disponibilidad/Falla en los datos de respaldos	Suplantación de identidad, préstamo de credenciales	Se cuenta con copias de seguridad del sistema	Multas o penalidades	Insignificante	Aceptar
22	Servidor SSH	Hardware	Uso Inadecuado de activos	Suplantación de identidad, préstamo de credenciales	Se cuenta con copias de seguridad del sistema.	Falta de trazabilidad Incumplimiento de leyes y regulaciones.	Menor	Aceptar
23	Servidor FTP	Hardware	Uso Inadecuado de activos	Multas o penalidades	Control de accesos de usuarios.	Pérdida económica. Transferencia de información por medios no seguros.	Menor	Aceptar
24	Servidor SQL	Hardware	Exposición de los medios de almacenamiento	Falta de trazabilidad	Se cuenta con copias de seguridad del sistema	Falta de trazabilidad	Moderado	Mitigar
25	File Server	Hardware	Uso Inadecuado de activos	Pérdida económica	Se cuenta con un control personalizado de carpetas.	Falta de trazabilidad	Moderado	Mitigar

26	Estaciones de trabajo	Hardware	Uso Inadecuado de activos	Transferencia de información por medios no seguros.	Se cuenta con copias de seguridad del sistema	Procesos judiciales	Menor	Aceptar
27	Dispositivo Móvil	Hardware	Uso Inadecuado de activos	Falta de trazabilidad	Se cuenta con copias de seguridad del sistema	Transferencia de información por medios no seguros	Menor	Aceptar
28	Disco duro externo	Hardware	Código troyano, virus	Falta de trazabilidad	Se cuenta con copias de seguridad del sistema.	Multas o penalidades	Moderado	Mitigar
29	Red de servicios	Comunicaciones	Fuga de información (divulgación, perdida o transferencia de información)	Procesos judiciales	Monitoreo de los registros de auditoría.	Incapacidad para prestar servicios.	Menor	Aceptar
30	WI-FI	Comunicaciones	Uso o conexión no autorizado / inapropiado de equipos y recursos informáticos / comunicaciones	Transferencia de información por medios no seguros	Se tiene un inventario de software autorizado.	Conexiones no autorizadas a la red	Insignificante	Aceptar
31	Proveedor de desarrollo	Servicios	Incumplimiento de contrato	Multas o penalidades	Se tiene un plan de mantenimiento preventivo y correctivo.	Incapacidad para prestar servicios.	Moderado	Mitigar
32	Proveedor de insumos	Servicios	Incumplimiento de contrato	Incapacidad para prestar servicios.	Se cuenta con control de accesos.	Incapacidad para prestar servicios.	Moderado	Mitigar

33	Personal	Recurso Humano	Robo de documentación/datos	Conexiones no autorizadas a la red	Se tiene un plan de mantenimiento preventivo y correctivo.	Perdida de personal calificado o fuga de talentos. Falta de capacitación en seguridad de la información.	Moderado	Mitigar
34	Oficinas	Infraestructura	Terremoto/Inundación/Incendio/Falla de suministro de respaldo (UPS)/Terrorismo	Incapacidad para prestar servicios.	Se cuenta con control de accesos.	Falta de planes de continuidad	Menor	Aceptar
35	Imagen institucional	Intangible	Terremoto/Inundación/Incendio/Falla de suministro de respaldo (UPS)/Terrorismo	Incapacidad para prestar servicios.	Sala de servidores con controles ambientales	Daños materiales	Menor	Aceptar
36	Cumplimiento	Intangible	Sanciones	Incumplimiento de leyes o regulaciones	Se tiene control de carpetas compartidas de algunas áreas.	Perdida de la imagen, reputación y nombre de la empresa. Multas o penalidades. Incumplimiento de leyes y regulaciones.	Menor	Aceptar

Fuente. Elaboración propia

9.11. Evaluación de Riesgos

Cuadro 45 Evaluación de riesgos

ID	Activos	Amenazas	Vulnerabilidad	Control Existente	Riesgo Asociado	Clasificación del Riesgo
12	SAP	Denegación de servicio	Falta de trazabilidad/ Fuga de información	Se cuenta con copias de seguridad del sistema.	Falta de trazabilidad/ Fuga de información Incumplimiento de leyes y regulaciones. Incumplimiento del Secreto de las Telecomunicaciones.	Catastrófico
24	Servidor SQL	Exposición de los medios de almacenamiento	Falta de trazabilidad	Se cuenta con copias de seguridad del sistema.	Falta de trazabilidad Incumplimiento de leyes y regulaciones.	Moderado
25	File Server	Uso Inadecuado de activos	Pérdida económica	Se cuenta con un control personalizado de carpetas.	Falta de trazabilidad	Moderado
2	Reportes de base de datos	Fuga de información (divulgación, perdida o transferencia de información)	Pérdida de oportunidades	No tiene controles.	Pérdida de oportunidades Incumplimiento de leyes y regulaciones.	Catastrófico
3	Actas de reuniones	Uso Inadecuado de activos	Perdida de la disponibilidad de la información	Se tiene un repositorio de todas reuniones realizadas desde el 2014.	Perdida de la disponibilidad de la información	Moderado
11	Sistema de registro	Denegación de servicio	Transacciones indebidas.	Se cuenta con copias de seguridad del sistema.	Incumplimiento de	Mayor

	de pedidos			Control de accesos de usuarios.	procedimientos internos	
5	Reportes	Fuga de información (divulgación, perdida o transferencia de información)	Perdida de la integridad de la información	No tiene controles.	Perdida de la integridad de la información	Moderado
31	Proveedor de desarrollo	Incumplimiento de contrato	Multas o penalidades	Se cuenta con un contrato de servicios.	Incapacidad para prestar servicios.	Moderado
32	Proveedor de insumos	Incumplimiento de contrato	Incapacidad para prestar servicios.	Se cuenta con un contrato de servicios.	Incapacidad para prestar servicios.	Moderado
33	Personal	Robo de documentación/datos	Conexiones no autorizadas a la red	Existe un plan de capacitación en seguridad de la información. - Existen acuerdos de confidencialidad, los cuales han sido entregados al personal al momento de su ingreso a la institución y estos acuerdos son firmados	Perdida de personal calificado o fuga de talentos. Falta de capacitación en seguridad de la información.	Moderado
28	Disco duro externo	Código troyano, virus	Falta de trazabilidad	Se cuenta con la autorización del área de Seguridad de la Información.	Multas o penalidades	Moderado
6	Contratos con Terceros	Fuga de información (divulgación, perdida o transferencia de información)	Pérdida económica	Se encuentra en revisión por área Legal.	Pérdida económica	Moderado

Fuente. Elaboración propia

9.12. Plan de Tratamiento de Riesgos

Cuadro 46 Plan de Tratamiento de Riesgos

ID	Activos	Riesgo Asociado	Clasificación del Riesgo	Estrategia	ISO /IEC27002	Detalle referencial del control	Detalles de las actividades a realizar	Responsable	Estado
12	SAP	Falta de trazabilidad/ Fuga de información Incumplimiento de Leyes y Regulaciones. Incumplimiento del Secreto de las Telecomunicaciones	Catastrófico	Mitigar	A.9.2.5	Revisión de los derechos de acceso a los usuarios	- Ejecutar el Procedimiento de Revisión de Derechos de Acceso. - Integrar los registros de auditoría a la plataforma de correlación de eventos. - Adecuación en el cumplimiento de la Ley 29733 Protección de Datos Personales y leyes aplicables.	Dueño del proceso	Pendiente
24	Servidor SQL	Falta de trazabilidad Incumplimiento de Leyes y Regulaciones. Incumplimiento del Secreto de las Telecomunicaciones	Moderado	Mitigar	A.12.4.3	Registros del administrador y operador	- Implementar los logs de auditoria con el Servidor SQL. - Integrar con la herramienta de correlación de eventos. - Ejecutar la Política de Administración de Servidores.	Dueño del proceso	Pendiente

							- Adecuación en el cumplimiento de la Ley 29733 Protección de Datos Personales y leyes aplicables.		
25	File Server	Inadecuado control de accesos	Moderado	Mitigar	A.9.2.1	Registro y cancelación de registro de usuario	- Revisar el cumplimiento del Procedimiento de Gestión de Accesos.	Dueño del proceso	Pendiente
2	Reportes de base de datos	Pérdida de oportunidades Incumplimiento de leyes y Regulaciones. Incumplimiento del Secreto de las Telecomunicaciones	Catastrófico	Mitigar	A.8.2.1	Clasificación de la información	- Implementar el formato de Clasificación de la Información. - Realizar la revisión perfiles y roles para extracción de reportes confidenciales.	Dueño del proceso	Pendiente
3	Actas de reuniones	Perdida de la disponibilidad de la información	Moderado	Mitigar	A.9.1.1	Política de control de acceso	- Difundir y/o ejecutar Procedimiento de Depuración de Carpetas Compartidas.	Dueño del proceso	Pendiente

11	Sistema de registro de pedidos	Incumplimiento de procedimientos internos	Mayor	Mitigar	A.9.2.1	Registro y cancelación de registro de usuario	- Revisar el cumplimiento del Procedimiento de Gestión de Accesos. - Ejecutar el Procedimiento de Revisión de Derechos de Accesos.	Dueño del proceso	Pendiente
5	Reportes	Perdida de la integridad de la información	Moderado	Mitigar	A.8.1.2	Propiedad de los activos	- Difundir y/o ejecutar Procedimiento de Depuración de Carpetas Compartidas.	Dueño del proceso	Pendiente
31	Proveedor de desarrollo	Incapacidad para prestar servicios.	Moderado	Mitigar	A.15.1.2	Abordar la seguridad dentro de los acuerdos del proveedor	- Verificar los contratos y acuerdos de confidencialidad.	Dueño del proceso	Pendiente
32	Proveedor de insumos	Incapacidad para prestar servicios.	Moderado	Mitigar	A.15.1.2	Abordar la seguridad dentro de los acuerdos del proveedor	- Verificar los contratos y acuerdos de confidencialidad.	Dueño del proceso	Pendiente
33	Personal	Perdida de personal calificado o fuga de talentos. Falta de capacitación en	Moderado	Mitigar	A.7.2.2	Concientización, educación y formación de seguridad de la	- Implementar un programa de Seguridad de la Información a todos los niveles de la empresa.	Dueño del proceso	Pendiente

		seguridad de la información.				información	- Actualizar los acuerdos de confidencialidad. - Solicitar el consentimiento de los usuarios para el cumplimiento de la Ley de Protección de Datos Personales.		
28	Disco duro externo	Multas o penalidades	Moderado	Mitigar	A.8.1.2	Propiedad de los activos	- Implementar el formato de Clasificación de la Información.	Dueño del proceso	Pendiente
6	Contratos con Terceros	Pérdida económica	Moderado	Mitigar	A.15.1.1	Política de seguridad de la información para las relaciones con el proveedor	- Validar los contratos con el área Legal	Dueño del proceso	Pendiente

Fuente. Elaboración propia.